JP 2000-057210

* NOTICES *

Japan Patent Office is not responsible for any

damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3. In the drawings, any words are not translated.

[Claim(s)]

[Claim 1] Since a ticket is stored, it is the approach of using an electron device, and it is the process which receives the 1st venue module relevant to the 1st venue. this -- with the process containing the 1st venue key for the 1st venue module checking the ticket to this 1st venue this -- with the process which checks the 1st venue module using the module loader key of this electron device The process which receives the 1st ticket to the event offered in this 1st venue, the process which receives the 1st ticket signature relevant to this 1st ticket -- this -- the 1st ticket signature -- this -- the approach of including the process attested using the 1st venue key, and the process which provides the check device of this 1st venue with this 1st ticket.

[Claim 2] the process which receives the 2nd venue module relevant to the 2nd venue -- it is -- this -- with the process containing the 2nd venue key for the 2nd venue module checking the ticket for this 2nd venue this -- with the process which checks the 2nd venue module using said module loader key The process which receives the 2nd ticket for the event offered in this 2nd venue, the process which receives the 2nd ticket signature using this 2nd ticket -- this -- the 2nd ticket signature -- this -- the approach according to claim 1 are the approach of including further the process attested using the 2nd venue key, and said 1st venue differs from this 2nd venue.

[Claim 3] the instruction by which it is the process which receives a share module, and this share module is used with said 1st venue module -- containing -- this -- the approach according to claim 1 of including further the process and the process which checks this share module using said module loader key which has a share venue key for checking the 1st venue module.

[Claim 4] The approach according to claim 3 each of said 1st venue module and said share module includes the process with which said process to check attests this module signature of said checked module using said module loader key including a module signature.

[Claim 5] The approach according to claim 3 of including further the process which checks said 1st venue module using said share venue key.

[Claim 6] The approach according to claim 1 the process which receives the 1st ticket includes the process which receives the challenge from a ticket loader, the process which signs this challenge using said 1st venue key, and the process which transmits the this signed challenge to this ticket loader.

BEST AVAILABLE COPY

[Claim 7] the process which receives the 1st venue module is related with the process which receives a series of 1st instruction for processing the ticket for the event in the 1st venue, the process which receive the 1st venue key for this 1st venue, and the process which store these the instructions of a series of to these the instructions of a series of -- this -- the approach according to claim 1 of including the process which stores the 1st venue key.

[Claim 8] The approach according to claim 7 of including further the process which judges whether the share module is stored on said electron device, and the process which receives this share module if this share module is not stored on this electron device.

[Claim 9] the process at which the process which receives said share module receives a series of 2nd instruction used with one or more venue modules -- this -- the process which receives the venue loader key for checking one or more venue modules -- this -- the process which stores a series of 2nd instruction -- this -- the approach according to claim 8 of including the process which stores this venue loader key relevant to a series of 2nd instruction.

[Claim 10] The approach according to claim 1 said process to check includes the process which attests the module signature of said 1st venue module using the module loader key of said electron device.

[Claim 11] The approach according to claim 1 of including further the process which cancels said 1st ticket.

[Claim 12] The approach according to claim 11 of including the process to which the process which cancels said 1st ticket makes this 1st ticket an invalid.

[Claim 13] The approach according to claim 1 of including further the process which makes said share module an invalid, and the process which receives this share module of a high version.

[Claim 14] the process which is the approach of maintaining the ticket for two or more venues in an electron device top, and stores the 1st venue module -- it is -- this -- the 1st venue module with the process containing the 1st venue key in relation to the 1st venue The 1st venue key is used. the process which receives a challenge from a ticket loader -- this -- The process which signs this challenge using the 1st digital signature, and the process which transmits the this signed challenge to this ticket loader, The process which receives the 1st electronic ticket for the entrance authorization to the event in this 1st venue, the process which receives the 1st ticket signature -- it is -- this -- the process relevant to this 1st electronic ticket in the 1st ticket signature -- this -- the 1st venue key -- using -- this -- the approach of including the process which attests the 1st ticket signature.

[Claim 15] the process which stores the 2nd venue module -- it is -- this -- the approach according to claim 14 are the approach the 2nd venue module includes the process containing the 2nd venue key further, and this 2nd venue differs from this 1st venue in relation to the 2nd venue.

[Claim 16] the process which receives the 2nd electronic ticket for the entrance authorization to the event in said 2nd venue, and the process which receives the 2nd ticket signature -- it is -- this -- the process relevant to this 2nd electronic ticket in the 2nd ticket signature, and said 2nd venue key -- using -- this -- the approach according to claim 15 of including further the process which attests the 2nd ticket signature.

[Claim 17] The approach according to claim 14 of being the process which judges whether the share module was stored and including further a process including the

instruction as which this share module is required with said 1st venue module, and the process in which this share module is not stored and which stores this share module if it becomes.

[Claim 18] The approach according to claim 14 of including the process which receives the random number with which the process which receives a challenge was generated.

[Claim 19] The approach according to claim 14 the process which receives the 1st electronic ticket includes the process which receives one or more details of the event in said 1st venue.

[Claim 20] The process which it is the approach of submitting a ticket, and this ticket is stored on the electron device which can store the ticket for two or more venues, and receives a challenge from a check device in a venue, How to include the process which signs this challenge using the 1st venue key, the process which transmits the this signed challenge to this check device, the process which receives the demand to the 1st ticket for the event which can set this venue, and the process which transmits this 1st ticket.

[Claim 21] The approach of claim 20 which includes further the process which said 1st ticket cancels.

[Claim 22] The approach according to claim 20 the process which receives a challenge includes the process which receives the generated random number.

[Claim 23] The approach according to claim 20 the process which transmits said 1st ticket includes the process which transmits one or more details which include this 1st ticket for said event.

[Claim 24] The 1st venue module for being ticket enclosure equipped with the memory device for storing, and processing the ticket for the event in the 1st venue, this -- with the device key for checking the 1st venue module, and the 1st ticket with which it is the 1st ticket for this event, and this ticket has a ticket signature It is an interface module for taking an interface with the 1st venue module. one of the venue key for attesting this ticket signature, and ticket loaders and check devices -- this -- Ticket enclosure sharable by two or more venue inter modules for storing an interface module.

[Claim 25] Equipment according to claim 24 further equipped with the 2nd venue module for processing the ticket for the event in the 2nd venue.

[Claim 26] Equipment according to claim 24 with which said ticket enclosure is equipped with a smart card.

[Claim 27] Equipment according to claim 24 with which said ticket enclosure is equipped with a pocket computer.

[Claim 28] The 1st venue module to be the storing medium including the DS for storing a ticket which can be computer read, and for this DS process the ticket for the event in the 1st venue, this -- with the device key for checking the 1st venue module, and the 1st ticket which is the 1st ticket for this event and has a ticket signature It is an interface module for taking an interface with the 1st venue module. one of the venue key for attesting this ticket signature, and ticket loaders and check devices -- this -- The storing medium sharable by two or more venue inter modules which can be equipped with interface module computer read.

[Claim 29] When performing by computer, it is the storing medium which stores the instruction which makes this computer perform the approach for processing an electronic ticket and which can be computer read. the process at which this approach receives the 1st venue module relevant to the 1st venue -- it is -- this -- with the process containing the

1st venue key for the 1st venue module checking the ticket to this 1st venue this -- with the process which checks the 1st venue module using the module loader key of this electronic storing device The process which receives the 1st ticket to the event offered in this 1st venue, the process which receives the 1st ticket signature using this 1st ticket -- this -- the 1st ticket signature -- this -- the storing medium which can be computer [which includes the process attested using the 1st venue key, and the process which provides the check device of this 1st venue with this 1st ticket] read.
[Claim 30] It is equipment for processing the ticket for the event in two or more venues. A receiving means to be a receiving means for receiving a module and to include a series of instructions for this module to process the ticket from an applet loader, Equipment equipped with the module check means for checking these a series of instructions, the ticket receiving means for receiving the ticket from a ticket loader, the ticket check means for checking this ticket, and the transmitting means for transmitting this ticket to a check device.

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the field of electronic commerce. The system and approach for the electronic ticket issue of banknotes are offered in more detail.
[0002]
[Description of the Prior Art] It is not a mechanical function strictly to use a ticket for sport holding, an amusement event, a travel, etc. any longer. The ticket issue-of-banknotes system has developed so that a computer system may be used in various phases of generation of a ticket, issue, and a check.
[0003] For example, in U.S. Pat. No. 5,598,477 indicated by Berson, a customer submits the information (for example, schedule data about airmail) about a desired ticket. Data processing system transmits ticket issue-of-banknotes information and the enciphered check data to a local printing system. A local system prints the ticket containing the confirmed information encoded in the two-dimensional bar code. A customer presents a ticket at airmail use time of day, and a check system scans the bar code of a ticket, changes data into a digital gestalt from a physical gestalt, and checks a ticket there. If effective, a customer will receive a boarding pass, a baggage-claim tag, etc.
[0004]
[Problem(s) to be Solved by the Invention] However, the system of Berson still needs issue of the ticket of paper. Though natural, the ticket of paper receives a pickpocket, the duplication ticket issue of banknotes, destruction, loss, etc. Furthermore, the ticket generated by the system of Berson fits use of a limitation once inevitably. Tickets are physically collected, when using airmail. There are two more disadvantageous points in this system. Use of a two-dimensional bar code needs [1st] the bar code scanner which can read the printer and such a bar code which can print such a bar code. Depending on the number of the locations where a ticket is printed or received, this can serve as remarkable cost. An advanced key managerial system is needed in use of the cryptographer stage which makes [2nd] confirmed information insurance.
[0005] In deformation of a Berson system, a big random number may be used instead of the security in a code. A specific random number is chosen and it is printed as a 1-

dimensional bar code on a physical ticket. Use of a large number reduces remarkably the probability for people to guess correctly right the number assigned to the specific ticket to separate events (airmail, amusement event, etc.). A random number is stored in a database accessible in the location where a ticket is used. When shown in a location with a ticket, the number on the ticket is compared with the list of effective numbers stored in the database. This system still includes the disadvantageous point of a proper in the ticket of papers, such as destruction, the duplication ticket issue of banknotes, and a limit of single use. In addition, if the further protection cannot be found, the database of a random number will give the brittleness of one point. Probably those who have access to a database can generate the ticket of a lot of falses.

[0006] In addition to the above-mentioned disadvantageous point, a well-known ticket issue-of-banknotes system permits the entrance only to one event or one location. Moreover, the ticket of the paper published by the known system is not changed into generally physically not replacing the published ticket. In other words, those who think that he wants to visit two or more event or two or more venues, to enjoy oneself, or to carry out have to bring and present a different ticket to each event or a venue. if a plan to visit more events or venues is carried out, the ticket of the further paper will be purchased and brought -- if it kicks, it will not become, therefore the risk of loss will become large.

[0007] Therefore, the purpose of this invention is that the system and approach for storing the electronic ticket to the event offered on single electron devices (a smart card, pocket computer, etc.) in two or more venues are offered.

[0008]

[Means for Solving the Problem] The approach by this invention is the approach of using an electron device, since a ticket is stored. the process which receives the 1st venue module relevant to the 1st venue -- it is -- this -- with the process containing the 1st venue key for the 1st venue module checking the ticket to this 1st venue this -- with the process which checks the 1st venue module using the module loader key of this electron device The process which receives the 1st ticket to the event offered in this 1st venue, the process which receives the 1st ticket signature relevant to this 1st ticket -- this -- the 1st ticket signature -- this -- the above-mentioned purpose is attained by the approach of including the process attested using the 1st venue key, and the process which provides the check device of this 1st venue with this 1st ticket.

[0009] the process which receives the 2nd venue module relevant to the 2nd venue in said approach -- it is -- this -- with the process containing the 2nd venue key for the 2nd venue module checking the ticket for this 2nd venue this -- with the process which checks the 2nd venue module using said module loader key The process which receives the 2nd ticket for the event offered in this 2nd venue, the process which receives the 2nd ticket signature using this 2nd ticket -- this -- the 2nd ticket signature -- this -- it is the approach of including further the process attested using the 2nd venue key, and said 1st venue may differ from this 2nd venue.

[0010] the instruction by which said approach is a process which receives a share module, and this share module is used with said 1st venue module -- containing -- this -- the process and the process which checks this share module using said module loader key which has a share venue key for checking the 1st venue module may be included further.

[0011] Each of said 1st venue module and said share module may include the process with which said process to check attests this module signature of said checked module using said module loader key including a module signature.
[0012] Said approach may include further the process which checks said 1st venue module using said share venue key.
[0013] The process which receives the 1st ticket may include the process which receives the challenge from a ticket loader, the process which signs this challenge using said 1st venue key, and the process which transmits the this signed challenge to this ticket loader.
[0014] the process which receives the 1st venue module is related with the process which receives a series of 1st instruction for processing the ticket for the event in the 1st venue, the process which receives the 1st venue key for this 1st venue, and the process which stores these the instructions of a series of to these the instructions of a series of -- this -- the process which stores the 1st venue key may include.
[0015] Said approach may include further the process which judges whether the share module is stored on said electron device, and the process which receives this share module if this share module is not stored on this electron device.
[0016] the process at which the process which receives said share module receives a series of 2nd instruction used with one or more venue modules -- this -- the process which receives the venue loader key for checking one or more venue modules -- this -- the process which stores a series of 2nd instruction -- this -- the process which stores this venue loader key relevant to a series of 2nd instruction may include.
[0017] Said process to check may include the process which attests the module signature of said 1st venue module using the module loader key of said electron device.
[0018] Said approach may include further the process which cancels said 1st ticket.
[0019] The process which cancels said 1st ticket may include the process which makes this 1st ticket an invalid.
[0020] Said approach may include further the process which makes said share module an invalid, and the process which receives this share module of a high version.
[0021] the process which is the approach of maintaining the ticket for two or more venues in an electron device top, and stores the 1st venue module -- it is -- this -- the 1st venue module with the process containing the 1st venue key in relation to the 1st venue The 1st venue key is used. the process which receives a challenge from a ticket loader -- this -- The process which signs this challenge using the 1st digital signature, and the process which transmits the this signed challenge to this ticket loader, The process which receives the 1st electronic ticket for the entrance authorization to the event in this 1st venue, the process which receives the 1st ticket signature -- it is -- this -- the process relevant to this 1st electronic ticket in the 1st ticket signature -- this -- the 1st venue key -- using -- this -- the above-mentioned purpose is attained by the approach of including the process which attests the 1st ticket signature.
[0022] the process in which said approach stores the 2nd venue module -- it is -- this -- the 2nd venue module is the approach of including the process containing the 2nd venue key further in relation to the 2nd venue, and this 2nd venue may differ from this 1st venue.
[0023] the process which receives the 2nd electronic ticket for the entrance authorization to an event [in / in said approach / said 2nd venue], and the process which receives the 2nd ticket signature -- it is -- this -- the process relevant to this 2nd electronic ticket in the

2nd ticket signature, and said 2nd venue key -- using -- this -- the process which attests the 2nd ticket signature may be included further.

[0024] Said approach is a process which judges whether the share module was stored, and may include further a process including the instruction as which this share module is required with said 1st venue module, and the process in which this share module is not stored and which stores this share module if it becomes.

[0025] Said approach may include the process which receives the random number with which the process which receives a challenge was generated.

[0026] The process at which said approach receives the 1st electronic ticket may include the process which receives one or more details of the event in said 1st venue.

[0027] The process which it is the approach of submitting a ticket, and this ticket is stored on the electron device which can store the ticket for two or more venues, and receives a challenge from a check device in a venue, The process which signs this challenge using the 1st venue key, and the process which transmits the this signed challenge to this check device, The above-mentioned purpose is attained by the approach of including the process which receives the demand to the 1st ticket for the event which can set this venue, and the process which transmits this 1st ticket.

[0028] Said approach may include further the process which said 1st ticket cancels.

[0029] The process which receives a challenge may include the process which receives the generated random number.

[0030] The process which transmits said 1st ticket may include the process which transmits one or more details which include this 1st ticket for said event.

[0031] The 1st venue module for being ticket enclosure equipped with the memory device for storing, and processing the ticket for the event in the 1st venue, this -- with the device key for checking the 1st venue module, and the 1st ticket with which it is the 1st ticket for this event, and this ticket has a ticket signature It is an interface module for taking an interface with the 1st venue module. one of the venue key for attesting this ticket signature, and ticket loaders and check devices -- this -- The above-mentioned purpose is attained by the ticket enclosure sharable by two or more venue inter modules for storing an interface module.

[0032] Said equipment may be further equipped with the 2nd venue module for processing the ticket for the event in the 2nd venue.

[0033] Said ticket enclosure with which said ticket enclosure may be equipped with a smart card may be equipped with a pocket computer.

[0034] The 1st venue module to be the storing medium including the DS for storing a ticket which can be computer read, and for this DS process the ticket for the event in the 1st venue, this -- with the device key for checking the 1st venue module, and the 1st ticket which is the 1st ticket for this event and has a ticket signature It is an interface module for taking an interface with the 1st venue module. one of the venue key for attesting this ticket signature, and ticket loaders and check devices -- this -- The above-mentioned purpose is attained by the storing medium sharable by two or more venue inter modules which can be equipped with interface module computer read.

[0035] When performing by computer, it is the storing medium which stores the instruction which makes this computer perform the approach for processing an electronic ticket and which can be computer read. the process at which this approach receives the 1st venue module relevant to the 1st venue -- it is -- this -- with the process containing the

1st venue key for the 1st venue module checking the ticket to this 1st venue this -- with the process which checks the 1st venue module using the module loader key of this electronic storing device The process which receives the 1st ticket to the event offered in this 1st venue, the process which receives the 1st ticket signature using this 1st ticket -- this -- the 1st ticket signature -- this -- with the process attested using the 1st venue key The above-mentioned purpose is attained by the storing medium which can be computer [which includes the process which provides the check device of this 1st venue with this 1st ticket] read.

[0036] It is equipment for processing the ticket for the event in two or more venues. A receiving means to be a receiving means for receiving a module and to include a series of instructions for this module to process the ticket from an applet loader, The module check means for checking these a series of instructions, and the ticket receiving means for receiving the ticket from a ticket loader, The above-mentioned purpose is attained by equipment equipped with the ticket check means for checking this ticket, and the transmitting means for transmitting this ticket to a check device.

[0037] In one embodiment of this invention, the system and approach for storing the electronic ticket to the event offered on single electron devices (a smart card, pocket computer, etc.) in two or more venues are offered. In this embodiment, an electron device receives the venue module relevant to each venue where a ticket is purchased, and is stored. The venue key for a venue module making it possible to store the ticket to the venue where the electron device was related, and checking each ticket is included. An electron device receives and stores the ticket issue-of-banknotes share module which includes the instruction demanded with one or more venue modules again. A ticket issue-of-banknotes share module contains the "venue loader key" for checking the installed venue module.

[0038] After an electron device is constituted using a ticket issue-of-banknotes share module and one or more venue modules, the ticket to the each installed venue module may be stored. In this embodiment of this invention, the user of an electron device specifies the parameters (an event, a date, time of day, seat, etc.) to a ticket, and a corresponding electronic ticket downloads from a ticket loader with a ticket signature. The venue key is used for the venue module to a corresponding venue module, and it attests the signature of the each stored ticket.

[0039] When it is what is shown for the entrance authorization to an event of a ticket, when a check device publishes a challenge code, an electron device is challenged in this embodiment. The venue module to the venue of an event answers a letter in the code signed and signed in the code using a venue key. After a signature is checked, an electron device transmits the ticket to an event and a ticket is canceled.

[0040]

[Embodiment of the Invention] By the following publications, this contractor can create and use this invention. The following publications are given according to a specific application and its demand. the operative condition this invention is indicated to be by this detail letter -- although it is not meant so that it may be limited like, the largest range adjusted with the principle and the description which are indicated by this detail letter is followed.

[0041] For example, in this embodiment of this invention, a cryptographer stage is used in order to ensure the safety of the electronic ticket loaded on a smart card and a venue

module, or applets (small-scale Java application etc.). This contractor is for the purpose of the cryptographic key indicated below to ensure the informational safety and the authentication nature which were stored on the smart card, and if he does not point out especially, he understands that it is not necessarily dependent on a specific code system. Therefore, various cryptographic keys are indicated below for the various purposes. However, this invention is not limited to the specific approach for the safety of a code, but an unsymmetrical key system, an object key system, or some alien systems [like] that may be devised can be used for the specific embodiment of this invention.

[0042] According to one embodiment of this invention, the system and approach for generating, storing and checking the electronic ticket to two or more venues are given. A ticket is 3COM although stored on a standard smart card in instantiation. PalmPilot or Dallas by Corporation Other devices, such as iButton by Semiconductor, are meant. The stored ticket may receive the opportunity of arbitration for an admission ticket or passing tickets, such as a sport event, an amusement event, airmail, and an automobile toll, to be purchased beforehand. Each venue where the ticket was stored on smart according to this embodiment of this invention has the related applet stored on the smart card. A ticket issue-of-banknotes share applet is stored again. These applets are used in order to take the interface between a smart card, and a ticket / venue load function and between a smart card and a ticket check device, so that it may be indicated below.

[0043] Drawing 1 illustrates the instantiation-system by the embodiment of this invention for publishing, storing and checking the ticket stored on a user's smart card. A smart card 100 follows ISO7816 specification over a smart card in instantiation. Such a smart card can store various classes and amounts of electronic data for being taken out behind.

[0044] The applet loader 102 loads one or more applets to up to a smart card 100. The applet loaded to up to a smart card 100 by the applet loader 102 makes it possible to store the ticket to the venue relevant to the applet to which the smart card 100 was loaded. For example, one venue applet is San. Francisco It can respond to the game of the baseball held by Giants. Loading this applet enables a smart card 100 to store the ticket to a specific game or the game (for example, season pass) of a certain range. In instantiation, the applet loader 102 is constituted so that the applet about a single venue may be loaded. However, in another embodiment, the applet loader 102 loads an applet from two or more venues.

[0045] a venue applet (namely, applet relevant to each venue) -- in addition, since a ticket issue-of-banknotes share applet is used by all venue applets, it is loaded to up to a smart card 100 again. In common with each of a venue applet, this share applet is available and gives the function used instead of each of a venue applet so that it may argue below.

[0046] The ticket loader 104 loads the electronic ticket to each event (or event of a certain range) to up to a smart card 100. Each smart card can store two or more tickets which receive a the same and different event, a venue, a date, etc. Each ticket loaded to up to the smart card 100 is stored in instantiation in relation to the venue applet corresponding to the venue which holds an event and receives a ticket. In this embodiment, before a ticket [as opposed to the event in the venue in the applet of a venue] is loaded, it is loaded on a smart card 100 (applet loader 102 etc.).

[0047] In instantiation, the ticket check device 106 is located in the venue which holds an event, and the ticket to the event is stored in a smart card 100. The check device 106

checks a ticket so that it may guarantee that a ticket is a thing to a current event, and it receives a ticket based on this check.

[0048] It is the separate electronic system which it had in order that it might set in this embodiment of this invention and the applet loader 102, the ticket loader 104, and the check device 106 might receive, read and write in a smart card 100. In this embodiment, a user shows each system a smart card 100 physically, in order to process a request. In another embodiment, the applet loaders 102, the ticket loaders 104, and all the check all [either or] 106 arrange to the same system. Especially, an applet loader and a ticket loader are so.

[0049] still more nearly another operative condition of this invention -- it sets like and the applet loaders 102, the ticket loaders 104, and all the check all [either or] 106 are equipped with the computer system connected to the Internet or other Wide Area Networks. It sets in such the embodiment and these systems are accessed by the user through a user's computer system which it had in order to receive, read and write in a smart card 100.

[0050] Drawing 2 illustrates the smart card 100 in which a ticket issue-of-banknotes share applet, two or more venue applets, and two or more tickets exist. A smart card 100 takes other devices (the applet loader 102, the ticket loader 104, the check device 106, etc. of drawing 1) and interfaces, and is equipped with the operating system 200 for managing the ejection of the information from a smart card, and storing. An operating system 200 is Java for operating the loaded applet in the embodiment illustrated. Virtual Machine (JVM) is included. An operating system 200 contains further cryptographic key 200a (called an "applet loader key" below) for checking the applet loaded to up to the smart card 100. Therefore, when an applet is loaded, the applet signatures 202b, 210b, and 220b use applet loader key 200a, and are attested. An applet signature is created by before loading of the related applet, or it and coincidence in instantiation.

[0051] The ticket issue-of-banknotes share applet 202 includes the instruction (for example, the gestalt of a module, an object, a function, etc. is taken) demanded by the various venue applets installed on the smart card 100. The ticket issue-of-banknotes share applet 202 enables size of each venue applet to give functions (protocol for communicating with a ticket check, the ticket loader 104, and the check device 106 etc.) common to each venue applet, therefore to become smaller, therefore can secure a storing field on a smart card 100. For example, in one embodiment of this invention, the ticket issue-of-banknotes share applet 202 gives the instruction for carrying out loading, check, and/or cancellation (for example, cancellation in order to obtain the entrance authorization to an event, after the ticket was used) for a ticket. The ticket issue-of-banknotes share applet 202 contains cryptographic key 202a (called a "venue loader key" below), in order to check each venue applet so that it may be described below. When a venue applet is loaded especially, the ticket issue-of-banknotes share applet 202 attests the venue signature of each applet.

[0052] In another embodiment of this invention, compulsion or the instruction for ensuring is included for a ticket issue-of-banknotes share applet observing the detail of a ticket. For example, in such an embodiment, a smart card 100 may be inserted in the smart card reading machine arranged in the seat-for-audience area in an event, in order that a user may confirm sitting on one's seat decided with the ticket or may assist finding a right seat.

[0053] Signs that the venue applets 210 and 220 are installed on the smart card 100 are shown. The venue applet 210 is SanFrancisco in instantiation. The game of the baseball in the home of Giants is expressed. The venue applet 220 is United in instantiation. The airmail of Airlines is expressed. The venue applets 210 and 220 contain the cryptographic keys 210a and 220a (called a "venue key" below) used in order to attest the venue applets 210 and 220 to the ticket loader 104 before loading a ticket. A venue key is used in order to check the ticket signature accompanying a ticket to the related venue again.
[0054] The venue applets 210 and 220 include the applet signatures 210b and 220b for checking a venue applet to an operating system 200 again. as mentioned above, instantiation ---like -- an applet signature -- before loading of a venue applet -- or it is created by it, simultaneously the applet loader 102. Next, when an applet is loaded, applet loader key 200a is used for an operating system 200, and it attests the applet signatures 210b and 220b.
[0055] The venue applets 210 and 220 include further the venue signatures 210c and 220c for checking a venue applet to a ticket issue-of-banknotes share applet. the applet signatures 210b and 220b -- the same -- the venue signatures 210c and 220c -- before the venue applet 210 and install of 220 -- or it -- simultaneously, it is created. When a venue applet is loaded, the ticket issue-of-banknotes share applet 202 attests a venue signature.
[0056] Tickets 212, 214, and 216 are San. Francisco The game of the specific baseball performed at the home of Giants is expressed. A ticket 222 is San. The specific airmail offered by UnitedAirlines to Pittsburgh from Francisco and PA is expressed.
[0057] Each ticket stored on the smart card 100 includes the information about a related event. Therefore, tickets 212, 214, and 216 include information, such as a date of a game, a waging-war partner, and the assignment seat number. In this embodiment of this invention, the information stored in the ticket is used with a ticket signature, in order to check authentication of a ticket. Therefore, the informational amount and informational class which were stored in the ticket change depending on a venue, an event, the class of ticket, etc. The owner of a smart card 100 may have the only ticket of the gestalt of for example, season pass instead of each tickets 212, 214, and 216. Exceeding one day, the season pass ticket is effective, therefore includes different information from tickets 212, 214, and 216.
[0058] Tickets 212, 214, 216, and 222 include the ticket signature (expressed by reference marks 212a, 214a, 216a, and 222a) generated by the ticket loader 104 using the corresponding key of a venue, respectively. the operative condition of this invention whose venue keys 210a and 220a are venue public keys using public key encryption (PKE) and an unsymmetrical key pair -- it sets like and a ticket signature is generated using the private key corresponding to a public key. In another embodiment which uses object keys (DES etc.), the ticket loader 104 signs the published ticket using the copy of the venue keys 210a and 220a. As mentioned above, when a ticket is loaded to up to a smart card 100, a corresponding venue applet checks a ticket by attesting a ticket signature using the venue key.
[0059] This contractor understands that the applet stored on the smart card 100 cannot access to the applet in which the secret of data could be held, therefore others were stored. This prevents that one applet commits or inspects injustice at the ticket relevant to a specific venue applet. However, in this embodiment, after being shown to the check

device 106, cancellation or use of a ticket is made improper. It sets in the another embodiment, and each ticket is deleted or overwritten.

[0060] In this embodiment of load this invention of an applet, the venue applet and ticket issue-of-banknotes share applet which are loaded on a smart card 100 contain the module of the computer code in which the computer program which can be performed or activation is possible. In this embodiment of this invention, the ticket issue-of-banknotes share applet is substantially the same between smart cards. The venue applet of each venue is the same between smart cards similarly except for a venue key and the ticket of arbitration which may be loaded.

[0061] In one embodiment of this invention, a venue applet contains the Java application constituted by the standard approach. For example, in order to form a binary class file, a file including a Java programming instruction uses a Java compiler, and is compiled. Next, a class file is changed into a smart card application file. Into this translation process, a card application file is signed in digital one using applet loader key 200a (shown in drawing 2), or its complementary depending on the class (for example, symmetry or asymmetry) of encryption.

[0062] Drawing 3 illustrates the instantiation-process by which the signed card application file (for example, applet 210 of drawing 2) is loaded from the applet loader 102 to up to a smart card 100. In this embodiment of this invention, the applet loader 102 is a ticket vending machine, and is arranged in the same location as the ticket loader 104. In this embodiment, the venue applet 210 is automatically loaded, if there is still no applet on a smart card 100 when the baseball ticket of Giants is purchased. Moreover, in this embodiment, the ticket issue-of-banknotes share applet 202 is automatically loaded, if there is nothing on a smart card 100. In another embodiment, when the time of a smart card being manufactured for both the ticket issue-of-banknotes share applet 202, and venue both [either or] 210 or it is sold, it is beforehand loaded on a smart card.

[0063] When drawing 3 is referred to here, a condition 300 is in an initiation condition. In a condition 302, it is combined with a smart card 100 and the applet loader 102 makes the preparations which download an applet 210. In instantiation, the owner of a smart card 100 inserts a smart card in the device containing the applet loader 102, and chooses install of an applet 210 (for example, thing for which the purchase of the baseball ticket of Giants is wished). In another embodiment, an owner inserts a smart card 100 in the separate computer system connected to the applet loader 102 through the Internet or other communication links.

[0064] In a condition 304, a smart card 100 shows that the preparation which loads an applet was made, and passes the information (Java Virtual Machine [the operating system of which applet is loaded and which version, and] are installed, information) concerning [on this embodiment and] a current configuration to an applet loader. In one embodiment, a smart card 100 performs a self-check, before showing what was been ready to receive an applet. In instantiation, a self-check examines the capacity of storing and the card to take out for data, and examines the memory cell which is a defect and which has ****** again. The information transmitted to the applet loader 102 by the smart card may contain the amount of the storing field which can be used on a card. An error message is shown to a user when the field for loading the selected applet is inadequate.

[0065] In a condition 306, the applet loader 102 judges whether the ticket issue-of-banknotes share applet 202 already exists on a smart card 100. As mentioned above, the ticket issue-of-banknotes share applet 202 includes the instruction used by the venue applet 210 and other venue applets. This decision is made in instantiation based on the information returned by the smart card 100 in the condition 304 to the applet loader 102.
[0066] When it is judged that the ticket issue-of-banknotes share applet 202 is not installed on a smart card 100 in a condition 306, a process continues to a condition 310. When that is not right, it is judged whether in the condition 308, the venue applet 210 is already loaded on the smart card 100. If not loaded, a process progresses to a condition 316. However, if both applets are already loaded, a process will progress to exit status 320.
[0067] In a condition 310, if the ticket issue-of-banknotes share applet is not signed yet, it is signed by applet loader key 200a using a complementary cryptographic key (for example, when using an unsymmetrical code system, a "secret" key corresponds to "open" key 200a) (for example, applet loader 102), and creates applet signature 202b (refer to drawing 2). Next, the signed applet is downloaded to a smart card 100. In instantiation, what byte of applet is downloaded and stored on a smart card by two or more of those streams (for example, inside of each stream about 200 bytes), and each stream is checked by the related checksum. In a condition 312, a smart card checks exact reception of an applet and notifies to an applet loader whether install succeeded in the condition 314, or it has not carried out. If the share applet 202 was not loaded surely, an error message will be returned and a process will be ended by exit status 320.
[0068] If the venue applet 210 is not loaded and it will be judged in a condition 308 if install of the ticket issue-of-banknotes share applet 202 is successful or, a process will progress to a condition 316.
[0069] In a condition 316, the venue applet 210 is signed by the applet loader 102 (if not signed yet), and creates applet signature 210b and/or venue signature 210c, and then downloads them from the applet loader 102 to up to a smart card 100. Venue key 210a is used in order to attest the venue applet 210 to the ticket loader 104, and in order to check the ticket loaded from the ticket loader, so that it may argue below. Depending on the class (for example, the symmetry or an unsymmetrical key) of desirable code safety, applet signature 210b and venue signature 210c are created, using respectively applet loader key 200a and venue loader 202a, or its complementary.
[0070] In a condition 318, a smart card 100 checks the downloaded applet and shows an applet loader whether loading of an applet was successful, or the error occurred. A smart card 100 checks in instantiation that reception of an applet has been successful by comparing with the checksum to which the checksum was calculated and it was given by the applet loader 102. In another embodiment, applet signature 210b of the downloaded applet is checked using the code technique corresponding to the gestalt of the key used for creation of a signature. In such one specific embodiment, a smart card 100 calculates the hash value from an applet, and compares the value with the hash value taken out from the signature. If these two hash values are in agreement, a smart card will think that the applet was received by the sound condition. A ticket signature is checked, when the same process is used and a ticket downloads. Subsequently, a process is ended by exit status 302.

[0071] When the load 1 ******** applet of a ticket is loaded to up to a smart card 100, the ticket to the events (airmail offered by a game at a sporting event place or a game, and the airline) in the venue is purchased, and may be loaded similarly. In this embodiment of this invention, a venue applet, the ticket issue-of-banknotes share applet 202, and the related ticket of each other are combined, there are and they are loaded if needed from the combined ticket / applet loader.
[0072] Drawing 4 purchases the electronic ticket to the game (the venue applet 210 for this is installed) of the baseball of Giants from the ticket loader 104, and illustrates the instantiation-procedure for installing an electronic ticket on a smart card 100. In this embodiment of this invention, the ticket loader 104 is a part of web server connected to public communication channels, such as the Internet. A smart card 100 is combined with the computer system operated by the owner of a smart card 100 in this embodiment. This computer system is connected to the Internet again. A ticket is chosen using the interface over the web server of a venue, then, is downloaded through the Internet, and is stored on a smart card 100.
[0073] When drawing 4 is referred to here, a condition 400 is in an initiation condition. In a condition 402, the owner of a smart card 100 starts ticket purchase / load procedure. In one embodiment of this invention, an owner chooses the event which wishes to have [1st] a ticket. In the embodiment of description, the game of baseball is specified with the desired number and desired class of a seat here. as another example, an owner specifies the airmail (the date and time of day -- and probably a seat is included) with which an owner wishes to board to an aerial route line reservation surrogate. After the owner of a smart card chooses a venue/event and specifies the need matter or criteria of arbitration about the event, an owner signs reception of the ticket constituted such.
[0074] In a condition 404, in order to attest a smart card and/or the venue applet 210, the ticket loader 104 identifies itself and challenges a smart card 100. A challenge is "a Zero Knowledge Interactive Proof (zero knowledge proof)" which takes the gestalt of the random number transmitted to the smart card 100 by the ticket loader 104 in instantiation. The venue applet 210 is venue key 210a Used, generates a digital signature, and fills a challenge by returning a result to the ticket loader 104. In another embodiment, the venue applet 210 fills a challenge in a condition 406 by returning a result to the ticket loader 104 by enciphering a random number using venue key 210a.
[0075] In a condition 408, the ticket loader 104 checks the signature received from the smart card 100. For the purpose of this check, the ticket loader 104 has the key of a complementary to venue key 210a. For example, in the embodiment of this invention which uses an unsymmetrical key (for example, RSA) which is the public key of the venue where venue key 210a is related, the ticket loader 104 has a corresponding private key. the operative condition of this invention which uses a symmetry key (for example, digital code criteria) -- setting like, the ticket loader 104 and the venue applet 210 have the copy of the same key. If the attempt of a check goes wrong, depending on the relation between operation and safety, it will fail and a ticket load process will perform whether challenge/check procedure is tried again or an error is reported (to the count of a limit).
[0076] Next, in a condition 410, the ticket loader 104 generates and signs the ticket 212 to a venue based on the event data chosen by the owner/user of a smart card. The ticket loader 104 signs a ticket 212 in instantiation using the same key as the venue applet 210

having been checked in the condition 408. In a condition 412, the ticket 212 which completed the signature by signature 212a is downloaded and stored on a smart card 100.
[0077] In a condition 414, by attesting signature 212a using venue key 210a, the venue applet 210 checks the downloaded ticket 212, and answers using the message which shows a success or failure in a condition 416. another operative condition of this invention -- it sets like and the 2nd different venue key from venue key 210a is stored with the venue applet 210 for the purpose which checks the downloaded ticket. Procedure is ended by exit status 418.
[0078] In the embodiment of description, each ticket must download from the ticket loader 104 here following the above-mentioned process. It sets in the another embodiment, and at once, to one venue, it chooses and processes and two or more tickets can download.
[0079] In this embodiment of ticket check this invention, a ticket is checked by the check device 106, when shown for reception in a suitable venue. Drawing 5 illustrates the instantiation-procedure for checking a ticket 212 by this embodiment of this invention.
[0080] A condition 500 is in an initiation condition. In a condition 502, a user presents a smart card 100 to the check device 106, in order to obtain the entrance authorization to the game of the baseball specified in a ticket 212. The check device 106 includes in instantiation the computer system constituted so that a smart card 100 might be communicated with reception and it.
[0081] In a condition 504, the check device 106 generates and publishes the challenge to a smart card 100, as carried out in the above-mentioned ticket load procedure. In a condition 506, venue key 210a is used for the random number given to a smart card 100, and it is signed by the venue applet 210. In a condition 508, a check device attests a signature to venue key 210a using the key of a complementary. By attesting the signature returned with the challenge, the check device 106 can check the venue applet 210.
[0082] After attesting a signature, in a condition 510, the check device 106 requires the ticket data held by the smart card 100. The venue applet 210 transmits a ticket 212 (for example, ticket data and a signature) to the check device 106 in a condition 512. Only the stored usable ticket is notified in instantiation to the current event from which the check device 106 is discriminated with the date, time of day, and/or other discernment data. In one embodiment of this invention, the ticket issue-of-banknotes share applet 202 determines the ticket specified to the check device 106 (for example, thing for which it is determined ticket - [which venue - therefore which venue applet, and] correspond to a check device). Or the venue applet 210 and the check device 106 communicate, in order to determine which [of two or more tickets in relation to a current venue] should be used.
[0083] In a condition 514, the check device 106 checks ticket data (for example, the date, time of day, a participating team, and the seat number are confirmed), and attests a ticket signature. If ticket data and a signature pass inspection, a smart card 100 will be ordered to cancel or eliminate a ticket 212, and a user will be permitted.
[0084] In the embodiment of description, a ticket 212 is overwritten here [of this invention] using the future ticket loaded on the smart card 100. As for a ticket, neither elimination nor overwrite is carried out in another embodiment.
[0085] The system and approach for storing and checking the electronic ticket for two or more venues on one smart card are offered. According to this embodiment, the operating

system of a smart card is Java. Virtual Machine and an applet loader key are included. The share applet containing a venue loader key is checked using an applet loader key, and is stored on a smart card. One or more venue applets are stored on a smart card with each venue key corresponding to a related venue again. Each venue applet is checked with an applet loader key and a venue loader key. A share applet is used by the venue applet in order to take an interface with a ticket loader and a ticket check device. A ticket is purchased to the event relevant to a venue applet, and is stored on a smart card in relation to a related venue applet. A ticket signature is attested using each venue applet venue key. A ticket is canceled, after being submitted in order to obtain the entrance authorization to an event.

[0086] The above-mentioned publication of the embodiment of this invention was shown for the purpose of only instantiation and explanation. Instantiation and a publication will not mean limiting to the gestalt which had this invention indicated, if all examples of all are not explained. Many alterations and modification are clear for this contractor. Therefore, it does not mean that the above-mentioned indication limits this invention, but the range of this invention is prescribed by the attached claim.

[0087]

[Effect of the Invention] The system and approach for storing the electronic ticket to the event offered on single electron devices (a smart card, pocket computer, etc.) in two or more venues are offered. The need is lost in issue of the ticket of paper, and when participating in many events, it becomes unnecessary thereby, to bring the ticket of much paper further.

[Brief Description of the Drawings]

[Drawing 1] It is one block diagram illustrating the system by the embodiment of this invention used since the ticket for the entrance to a venue applet and a venue of a smart card is stored.

[Drawing 2] It is drawing illustrating the smart card containing two or more venue applets and tickets by the embodiment of this invention.

[Drawing 3] It is the flow chart which shows the one approach by the embodiment of this invention of loading a venue applet on a smart card.

[Drawing 4] It is the flow chart which shows the one approach by the embodiment of this invention of loading a ticket on a smart card.

[Drawing 5] It is the flow chart which shows one method by the embodiment of this invention of checking the ticket stored on the smart card.

[Description of Notations]

100 Smart Card
102 Applet Loader
104 Ticket Loader
106 Check Device

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－57210
（P2000－57210A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ　15/21	Ａ	
// Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ	
	６６０		６６０Ａ	
			６６０Ｂ	

審査請求　未請求　請求項の数30　ＯＬ　（全 16 頁）

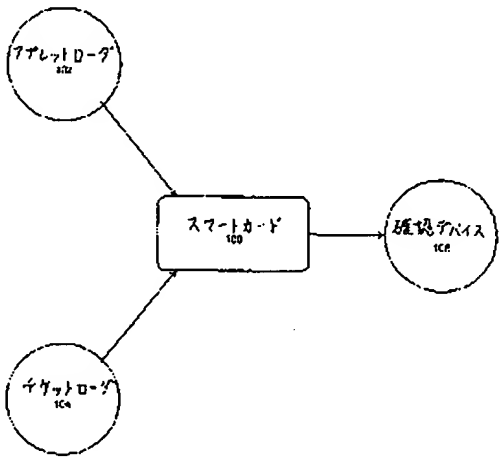
(21)出願番号　特願平11－180905
(22)出願日　平成11年６月25日(1999.6.25)
(31)優先権主張番号　０９／１０６．６００
(32)優先日　平成10年６月29日(1998.6.29)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　595034134
サン・マイクロシステムズ・インコーポレイテッド
Ｓｕｎ　Ｍｉｃｒｏｓｙｓｔｅｍｓ，　Ｉｎｃ．
アメリカ合衆国　カリフォルニア州　94303　パロ　アルト　サン　アントニオ　ロード　901
(74)代理人　100078282
弁理士　山本　秀策

最終頁に続く

(54)【発明の名称】　スマートカードを用いた多開催地チケット発券

(57)【要約】
【課題】　単一の電子デバイス（スマートカード，および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供されること。
【解決手段】チケットを格納するために電子デバイスを使用する方法であって、第１の開催地に関連する第１の開催地モジュールを受信する工程であって、第１の開催地モジュールが第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、第１の開催地モジュールを電子デバイスのモジュールローダ鍵を用いて確認する工程と、第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と、第１のチケットに関連する第１のチケット署名を受信する工程と、第１のチケット署名を第１の開催地鍵を用いて認証する工程と、第１のチケットを第１の開催地の確認デバイスに提供する工程と、を包含する方法が提供される。



1

【特許請求の範囲】

【請求項１】　チケットを格納するために電子デバイスを使用する方法であって．

第１の開催地に関連する第１の開催地モジュールを受信する工程であって、該第１の開催地モジュールが該第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、

該第１の開催地モジュールを該電子デバイスのモジュールローダ鍵を用いて確認する工程と．

該第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と．

該第１のチケットに関連する第１のチケット署名を受信する工程と、

該第１のチケット署名を該第１の開催地鍵を用いて認証する工程と、

該第１のチケットを該第１の開催地の確認デバイスに提供する工程と．を包含する方法。

【請求項２】　第２の開催地に関連する第２の開催地モジュールを受信する工程であって、該第２の開催地モジュールが該第２の開催地のためのチケットを確認するための第２の開催地鍵を含む．工程と．

該第２の開催地モジュールを前記モジュールローダ鍵を用いて確認する工程と、

該第２の開催地で提供されるイベントのための第２のチケットを受信する工程と．

該第２のチケットを用いて第２のチケット署名を受信する工程と、

該第２のチケット署名を該第２の開催地鍵を用いて認証する工程と、をさらに包含する方法であって、

前記第１の開催地が該第２の開催地と異なる、請求項１に記載の方法。

【請求項３】　共有モジュールを受信する工程であって．該共有モジュールが前記第１の開催地モジュールによって使用される命令を含み、該第１の開催地モジュールを確認するための共有開催地鍵を有する、工程と、

該共有モジュールを前記モジュールローダ鍵を用いて確認する工程と．をさらに包含する請求項１に記載の方法。

【請求項４】　前記第１の開催地モジュールおよび前記共有モジュールの各々がモジュール署名を含み．前記確認する工程が前記確認されたモジュールの該モジュール署名を前記モジュールローダ鍵を用いて認証する工程を包含する、請求項３に記載の方法。

【請求項５】　前記第１の開催地モジュールを前記共有開催地鍵を用いて確認する工程をさらに包含する．請求項３に記載の方法。

【請求項６】　第１のチケットを受信する工程が．

チケットローダからのチャレンジを受信する工程と、

該チャレンジを前記第１の開催地鍵を用いて署名する工程と．

2

該署名されたチャレンジを該チケットローダに送信する工程と、を包含する、請求項１に記載の方法。

【請求項７】　第１の開催地モジュールを受信する工程が．

第１の開催地におけるイベントのためのチケットを処理するための第１の一連の命令を受信する工程と．

該第１の開催地のための第１の開催地鍵を受信する工程と．

該一連の命令を格納する工程と、

該一連の命令に関連する該第１の開催地鍵を格納する工程と．を包含する請求項１に記載の方法。

【請求項８】　共有モジュールが前記電子デバイス上に格納されているかどうかを判断する工程と、

該共有モジュールが該電子デバイス上に格納されていなければ、該共有モジュールを受信する工程と、をさらに包含する請求項７に記載の方法。

【請求項９】　前記共有モジュールを受信する工程が、１つ以上の開催地モジュールによって使用される第２の一連の命令を受信する工程と、

該１つ以上の開催地モジュールを確認するための開催地ローダ鍵を受信する工程と．

該第２の一連の命令を格納する工程と．

該第２の一連の命令に関連する該開催地ローダ鍵を格納する工程と、を包含する．請求項８に記載の方法。

【請求項１０】　前記確認する工程が．前記第１の開催地モジュールのモジュール署名を前記電子デバイスのモジュールローダ鍵を用いて認証する工程を包含する、請求項１に記載の方法。

【請求項１１】　前記第１のチケットをキャンセルする工程をさらに包含する、請求項１に記載の方法。

【請求項１２】　前記第１のチケットをキャンセルする工程が該第１のチケットを無効にする工程を包含する、請求項１１に記載の方法。

【請求項１３】　前記共有モジュールを無効にする工程と．

新しいバージョンの該共有モジュールを受信する工程と．をさらに包含する、請求項１に記載の方法。

【請求項１４】　電子デバイス上で複数の開催地のためのチケットを維持する方法であって．

第１の開催地モジュールを格納する工程であって．該第１の開催地モジュールが第１の開催地と関連しそして第１の開催地鍵を含む、工程と、

チケットローダからチャレンジを受信する工程と．

該第１の開催地鍵を使用して、第１のデジタル署名を用いて該チャレンジを署名する工程と．

該署名されたチャレンジを該チケットローダに送信する工程と、

該第１の開催地におけるイベントに対する入場許可のための第１の電子チケットを受信する工程と、

第１のチケット署名を受信する工程であって、該第１の

チケット署名が該第１の電子チケットと関連する．工程と．

該第１の開催地鍵を用いて．該第１のチケット署名を認証する工程と．を包含する方法。

【請求項１５】　第２の開催地モジュールを格納する工程であって、該第２の開催地モジュールが第２の開催地と関連しそして第２の開催地鍵を含む．工程を．さらに包含する方法であって、

該第２の開催地が該第１の開催地と異なる、請求項１４に記載の方法。

【請求項１６】　前記第２の開催地におけるイベントに対する入場許可のための第２の電子チケットを受信する工程と、

第２のチケット署名を受信する工程であって、該第２のチケット署名が該第２の電子チケットと関連する．工程と．

前記第２の開催地鍵を用いて、該第２のチケット署名を認証する工程と．をさらに包含する請求項１５に記載の方法。

【請求項１７】　共有モジュールが格納されたかどうかを判断する工程であって．該共有モジュールが前記第１の開催地モジュールによって要求される命令を含む、工程と．

該共有モジュールが格納されていないならば、該共有モジュールを格納する工程と．をさらに包含する請求項１４に記載の方法。

【請求項１８】　チャレンジを受信する工程が生成された乱数を受信する工程を包含する、請求項１４に記載の方法。

【請求項１９】　第１の電子チケットを受信する工程が．前記第１の開催地におけるイベントの１つ以上の詳細を受信する工程を包含する、請求項１４に記載の方法。

【請求項２０】　チケットを提出する方法であって、該チケットが複数の開催地のためのチケットを格納することのできる電子デバイス上に格納され．

開催地において確認デバイスからチャレンジを受信する工程と、

第１の開催地鍵を使用して該チャレンジを署名する工程と．

該署名されたチャレンジを該確認デバイスに送信する工程と．

該開催地のおけるイベントのための第１のチケットに対する要求を受信する工程と．

該第１のチケットを送信する工程と．を包含する方法。

【請求項２１】　前記第１のチケットがキャンセルする工程をさらに包含する請求項２０の方法。

【請求項２２】　チャレンジを受信する工程が．生成された乱数を受信する工程を包含する．請求項２０に記載の方法。

【請求項２３】　前記第１のチケットを送信する工程が．前記イベントのための該第１のチケットを包含する１つ以上の詳細を送信する工程を包含する、請求項２０に記載の方法。

【請求項２４】　格納のためのメモリデバイスを備えるチケット格納装置であって．

第１の開催地におけるイベントのためのチケットを処理するための第１の開催地モジュールと．

該第１の開催地モジュールを確認するためのデバイス鍵と．

該イベントのための第１のチケットであって、該チケットがチケット署名を有する．第１のチケットと．

該チケット署名を認証するための開催地鍵と、

チケットローダおよび確認デバイスのうちの１つと該第１の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を格納するためのチケット格納装置。

【請求項２５】　第２の開催地におけるイベントのためのチケットを処理するための第２の開催地モジュールをさらに備える請求項２４に記載の装置。

【請求項２６】　前記チケット格納装置がスマートカードを備える、請求項２４に記載の装置。

【請求項２７】　前記チケット格納装置が携帯コンピュータを備える．請求項２４に記載の装置。

【請求項２８】　チケットを格納するためのデータ構造を含むコンピュータ読み出し可能格納媒体であって、該データ構造が．

第１の開催地におけるイベントのためのチケットを処理するための第１の開催地モジュールと．

該第１の開催地モジュールを確認するためのデバイス鍵と．

該イベントのための第１のチケットであって、チケット署名を有する．第１のチケットと、

該チケット署名を認証するための開催地鍵と、

チケットローダおよび確認デバイスのうちの１つと該第１の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を備える、コンピュータ読み出し可能格納媒体。

【請求項２９】　コンピュータによって実行される場合に．電子チケットを処理するための方法を該コンピュータに実行させる命令を格納するコンピュータ読み出し可能格納媒体であって、該方法が、

第１の開催地に関連する第１の開催地モジュールを受信する工程であって、該第１の開催地モジュールが該第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、

該第１の開催地モジュールを該電子格納デバイスのモジ

ュールローダ鍵を用いて確認する工程と、
該第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と、
該第１のチケットを用いて第１のチケット署名を受信する工程と、
該第１のチケット署名を該第１の開催地鍵を用いて認証する工程と、
該第１のチケットを該第１の開催地の確認デバイスに提供する工程と、を包含する、コンピュータ読み出し可能格納媒体。

【請求項３０】　複数の開催地におけるイベントのためのチケットを処理するための装置であって、
モジュールを受信するための受信手段であって、該モジュールがアプレットローダからのチケットを処理するための一連の命令を包含する、受信手段と、
該一連の命令を確認するためのモジュール確認手段と、
チケットローダからのチケットを受信するためのチケット受信手段と、
該チケットを確認するためのチケット確認手段と、
該チケットを確認デバイスに送信するための送信手段と、を備える装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子商取引の分野に関する。より詳しくは、電子チケット発券のためのシステムおよび方法を提供する。

【０００２】

【従来の技術】スポーツ開催、娯楽イベント、旅行などのためにチケットを使用することは、もはや厳密には機械的な機能ではない。チケット発券システムは、チケットの生成、発行、および確認作業のさまざまな段階においてコンピュータシステムを利用するように発展してきた。

【０００３】例えば、Ｂｅｒｓｏｎによって開示された、米国特許第５，５９８，４７７号において、顧客は、所望のチケットに関する情報（例えば、航空便に関する予定データ）を提出する。データ処理システムは、チケット発券情報および暗号化された確認データをローカル印刷システムに送信する。ローカルシステムは、２次元バーコード中に符号化された確認情報を含むチケットを印刷する。顧客は、航空便利用時刻にチケットを提示し、そこで確認システムは、チケットのバーコードをスキャンし、データを物理的形態からデジタル形態へ変換し、チケットを確認する。有効であるならば、顧客は、搭乗券および手荷物預かり証などを受け取る。

【０００４】

【発明が解決しようとする課題】しかし、Ｂｅｒｓｏｎのシステムは、紙のチケットの発行を依然必要とする。当然ながら、紙のチケットは、スリ、重複チケット発券、損壊、紛失などを被る。さらに、Ｂｅｒｓｏｎのシステムによって生成されるチケットは、必然的に１回限りの使用に適している。チケットは、航空便を利用するときに物理的に回収される。このシステムには、さらに２つの不利な点がある。第１に、２次元バーコードの使用は、そのようなバーコードを印刷することのできるプリンタおよびそのようなバーコードを読み取れることのできるバーコードスキャナを必要とする。チケットが印刷または受理される場所の数に依存して、これは著しいコストとなり得る。第２に、確認情報を安全にする暗号手段の使用では、高度な鍵管理システムを必要とする。

【０００５】Ｂｅｒｓｏｎシステムの変形においては、暗号によるセキュリティの代わりに大きな乱数が使用され得る。特定の乱数が選択され、物理的チケット上に１次元バーコードとして印刷される。大きな数を使用すると、別個のイベント（航空便、娯楽イベントなど）に対する特定のチケットに割り当てられる番号を人が正確に言い当てる確率は、著しく低下する。乱数は、チケットが使用される場所にアクセス可能なデータベース中に格納される。チケットがある場所で提示される場合、そのチケット上の番号は、データベース中に格納された有効番号のリストと比較される。このシステムは、損壊、重複チケット発券、および単一使用の制限などの紙のチケットに固有の不利な点を依然含んでいる。加えて、さらなる保護がなければ、乱数のデータベースは、一点の脆弱さを与える。データベースへアクセスを有する人が大量の偽のチケットをおそらく生成し得る。

【０００６】上記の不利な点に加えて、公知のチケット発券システムは、１つのイベントまたは１つの場所だけに対する入場を許可するものである。また、既知のシステムによって発行される紙のチケットは一般に、発行されたチケットを物理的に置き換えずには、変更されない。言い換えると、複数のイベントまたは複数の開催地を訪れたりまたは楽しんだりしたいと考える人は、各イベントまたは開催地に対する異なるチケットを持参し提示しなければならない。より多くのイベントまたは開催地を訪れる計画をすると、さらなる紙のチケットを購入し持参しなければならず、従って紛失の危険が大きくなる。

【０００７】従って、本発明の目的は、単一の電子デバイス（スマートカード、および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供されることである。

【０００８】

【課題を解決するための手段】本発明による方法は、チケットを格納するために電子デバイスを使用する方法であって、第１の開催地に関連する第１の開催地モジュールを受信する工程であって、該第１の開催地モジュールが該第１の開催地に対するチケットを確認するための第１の開催地鍵を含む、工程と、該第１の開催地モジュー

ルを該電子デバイスのモジュールローダ鍵を用いて確認する工程と、該第１の開催地で提供されるイベントに対する第１のチケットを受信する工程と．該第１のチケットに関連する第１のチケット署名を受信する工程と、該第１のチケット署名を該第１の開催地鍵を用いて認証する工程と、該第１のチケットを該第１の開催地の確認デバイスに提供する工程と．を包含する方法により．上記目的が達成される。

【０００９】前記方法は．第２の開催地に関連する第２の開催地モジュールを受信する工程であって、該第２の開催地モジュールが該第２の開催地のためのチケットを確認するための第２の開催地鍵を含む．工程と．該第２の開催地モジュールを前記モジュールローダ鍵を用いて確認する工程と．該第２の開催地で提供されるイベントのための第２のチケットを受信する工程と、該第２のチケットを用いて第２のチケット署名を受信する工程と、該第２のチケット署名を該第２の開催地鍵を用いて認証する工程と、をさらに包含する方法であって、前記第１の開催地が該第２の開催地と異なってもよい。

【００１０】前記方法は．共有モジュールを受信する工程であって、該共有モジュールが前記第１の開催地モジュールによって使用される命令を含み．該第１の開催地モジュールを確認するための共有開催地鍵を有する、工程と．該共有モジュールを前記モジュールローダ鍵を用いて確認する工程と、をさらに包含してもよい。

【００１１】前記第１の開催地モジュールおよび前記共有モジュールの各々がモジュール署名を含み、前記確認する工程が前記確認されたモジュールの該モジュール署名を前記モジュールローダ鍵を用いて認証する工程を包含してもよい。

【００１２】前記方法は．前記第１の開催地モジュールを前記共有開催地鍵を用いて確認する工程をさらに包含してもよい。

【００１３】第１のチケットを受信する工程が．チケットローダからのチャレンジを受信する工程と、該チャレンジを前記第１の開催地鍵を用いて署名する工程と、該署名されたチャレンジを該チケットローダに送信する工程と．を包含してもよい。

【００１４】第１の開催地モジュールを受信する工程が．第１の開催地におけるイベントのためのチケットを処理するための第１の一連の命令を受信する工程と、該第１の開催地のための第１の開催地鍵を受信する工程と．該一連の命令を格納する工程と．該一連の命令に関連する該第１の開催地鍵を格納する工程と、を包含してもよい。

【００１５】前記方法は．共有モジュールが前記電子デバイス上に格納されているかどうかを判断する工程と、該共有モジュールが該電子デバイス上に格納されていなければ、該共有モジュールを受信する工程と、をさらに包含してもよい。

【００１６】前記共有モジュールを受信する工程が、１つ以上の開催地モジュールによって使用される第２の一連の命令を受信する工程と．該１つ以上の開催地モジュールを確認するための開催地ローダ鍵を受信する工程と．該第２の一連の命令を格納する工程と、該第２の一連の命令に関連する該開催地ローダ鍵を格納する工程と．を包含してもよい。

【００１７】前記確認する工程が、前記第１の開催地モジュールのモジュール署名を前記電子デバイスのモジュールローダ鍵を用いて認証する工程を包含してもよい。

【００１８】前記方法は．前記第１のチケットをキャンセルする工程をさらに包含してもよい。

【００１９】前記第１のチケットをキャンセルする工程が該第１のチケットを無効にする工程を包含してもよい。

【００２０】前記方法は．前記共有モジュールを無効にする工程と、新しいバージョンの該共有モジュールを受信する工程と．をさらに包含してもよい。

【００２１】電子デバイス上で複数の開催地のためのチケットを維持する方法であって、第１の開催地モジュールを格納する工程であって．該第１の開催地モジュールが第１の開催地と関連しそして第１の開催地鍵を含む、工程と、チケットローダからチャレンジを受信する工程と．該第１の開催地鍵を使用して、第１のデジタル署名を用いて該チャレンジを署名する工程と、該署名されたチャレンジを該チケットローダに送信する工程と．該第１の開催地におけるイベントに対する入場許可のための第１の電子チケットを受信する工程と．第１のチケット署名を受信する工程であって、該第１のチケット署名が該第１の電子チケットと関連する、工程と、該第１の開催地鍵を用いて．該第１のチケット署名を認証する工程と．を包含する方法により．上記目的が達成される。

【００２２】前記方法は．第２の開催地モジュールを格納する工程であって、該第２の開催地モジュールが第２の開催地と関連しそして第２の開催地鍵を含む．工程を．さらに包含する方法であって、該第２の開催地が該第１の開催地と異なってもよい。

【００２３】前記方法は．前記第２の開催地におけるイベントに対する入場許可のための第２の電子チケットを受信する工程と．第２のチケット署名を受信する工程であって、該第２のチケット署名が該第２の電子チケットと関連する、工程と、前記第２の開催地鍵を用いて、該第２のチケット署名を認証する工程と．をさらに包含してもよい。

【００２４】前記方法は．共有モジュールが格納されたかどうかを判断する工程であって、該共有モジュールが前記第１の開催地モジュールによって要求される命令を含む．工程と．該共有モジュールが格納されていないならば．該共有モジュールを格納する工程と、をさらに包含してもよい。

【0025】前記方法は、チャレンジを受信する工程が生成された乱数を受信する工程を包含してもよい。

【0026】前記方法は、第1の電子チケットを受信する工程が、前記第1の開催地におけるイベントの1つ以上の詳細を受信する工程を包含してもよい。

【0027】チケットを提出する方法であって、該チケットが複数の開催地のためのチケットを格納することのできる電子デバイス上に格納され、開催地において確認デバイスからチャレンジを受信する工程と、第1の開催地鍵を使用して該チャレンジを署名する工程と、該署名されたチャレンジを該確認デバイスに送信する工程と、該開催地のおけるイベントのための第1のチケットに対する要求を受信する工程と、該第1のチケットを送信する工程と、を包含する方法により上記目的が達成される。

【0028】前記方法は、前記第1のチケットがキャンセルする工程をさらに包含してもよい。

【0029】チャレンジを受信する工程が、生成された乱数を受信する工程を包含してもよい。

【0030】前記第1のチケットを送信する工程が、前記イベントのための該第1のチケットを包含する1つ以上の詳細を送信する工程を包含してもよい。

【0031】格納のためのメモリデバイスを備えるチケット格納装置であって、第1の開催地におけるイベントのためのチケットを処理するための第1の開催地モジュールと、該第1の開催地モジュールを確認するためのデバイス鍵と、該イベントのための第1のチケットであって、該チケットがチケット署名を有する、第1のチケットと、該チケット署名を認証するための開催地鍵と、チケットローダおよび確認デバイスのうちの1つと該第1の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を格納するためのチケット格納装置により、上記目的が達成される。

【0032】前記装置は、第2の開催地におけるイベントのためのチケットを処理するための第2の開催地モジュールをさらに備えてもよい。

【0033】前記チケット格納装置がスマートカードを備えてもよい前記チケット格納装置が携帯コンピュータを備えてもよい。

【0034】チケットを格納するためのデータ構造を含むコンピュータ読み出し可能格納媒体であって、該データ構造が、第1の開催地におけるイベントのためのチケットを処理するための第1の開催地モジュールと、該第1の開催地モジュールを確認するためのデバイス鍵と、該イベントのための第1のチケットであって、チケット署名を有する、第1のチケットと、該チケット署名を認証するための開催地鍵と、チケットローダおよび確認デバイスのうちの1つと該第1の開催地モジュールとのインターフェースをとるためのインターフェースモジュールであって、複数の開催地モジュール間で共有可能である、インターフェースモジュールと、を備える、コンピュータ読み出し可能格納媒体により、上記目的が達成される。

【0035】コンピュータによって実行される場合に、電子チケットを処理するための方法を該コンピュータに実行させる命令を格納するコンピュータ読み出し可能格納媒体であって、該方法が、第1の開催地に関連する第1の開催地モジュールを受信する工程であって、該第1の開催地モジュールが該第1の開催地に対するチケットを確認するための第1の開催地鍵を含む、工程と、該第1の開催地モジュールを該電子格納デバイスのモジュールローダ鍵を用いて確認する工程と、該第1の開催地で提供されるイベントに対する第1のチケットを受信する工程と、該第1のチケットを用いて第1のチケット署名を受信する工程と、該第1のチケット署名を該第1の開催地鍵を用いて認証する工程と、該第1のチケットを該第1の開催地の確認デバイスに提供する工程と、を包含する、コンピュータ読み出し可能格納媒体により、上記目的が達成される。

【0036】複数の開催地におけるイベントのためのチケットを処理するための装置であって、モジュールを受信するための受信手段であって、該モジュールがアプレットローダからのチケットを処理するための一連の命令を包含する、受信手段と、該一連の命令を確認するためのモジュール確認手段と、チケットローダからのチケットを受信するためのチケット受信手段と、該チケットを確認するためのチケット確認手段と、該チケットを確認デバイスに送信するための送信手段と、を備える装置により、上記目的が達成される。

【0037】本発明の1つの実施態様において、単一の電子デバイス（スマートカード、および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供される。この実施態様において、電子デバイスは、チケットが購入される各開催地に関連した開催地モジュールを受信し格納する。開催地モジュールは、電子デバイスが、関連した開催地に対するチケットを格納することを可能にし、また個々のチケットを確認するための開催地鍵を含む。電子デバイスはまた、1つ以上の開催地モジュールによって要求される命令を含むチケット発券共有モジュールを受信し格納する。チケット発券共有モジュールは、インストールされた開催地モジュールを確認するための「開催地ローダ鍵」を含む。

【0038】電子デバイスがチケット発券共有モジュールおよび1つ以上の開催地モジュールを用いて構成された後に、各インストールされた開催地モジュールに対するチケットが格納され得る。本発明の本実施態様において、電子デバイスのユーザは、チケットに対するパラメ

ータ（イベント．日付、時刻、座席など）を特定し、対応する電子チケットがチケット署名とともにチケットローダからダウンロードされる。対応する開催地モジュールに対する開催地モジュールは、その開催地鍵を使用して．各格納されたチケットの署名を認証する。

【００３９】チケットがイベントへの入場許可のために提示されるものである場合．本実施態様においては、確認デバイスがチャレンジコードを発行することによって電子デバイスをチャレンジする。イベントの開催地に対する開催地モジュールは．開催地鍵を用いてそのコードを署名し、署名されたコードを返信する。署名が確認された後に、電子デバイスはイベントに対するチケットを転送し、チケットはキャンセルされる。

【００４０】

【発明の実施の形態】以下の記載により、当業者は、本発明を作成および使用することができる。以下の記載は．特定の用途およびその要求にしたがって与えられる。本発明は．本明細書中で示される実施態様に限定されるように意図されないが．本明細書中で開示される原理および特徴に整合する最も広い範囲に従うものである。

【００４１】例えば、本発明の本実施態様において、暗号手段は、スマートカード上にロードされる電子チケットおよび開催地モジュールまたはアプレット（小規模Ｊａｖａアプリケーションなど）の安全性を確実にするために用いられる。当業者は．以下に記載される暗号鍵の目的が、スマートカード上に格納された情報の安全性および認証性を確実にするためであり．特に指摘しなければ必ずしも特定の暗号システムに依存しないことを理解する。したがって、種々の暗号鍵は．種々の目的のために以下に記載される。しかし、本発明は、暗号の安全性のための特定の方法に限定されず、本発明の特定の実施態様は、非対称鍵システム．対象鍵システム、または工夫され得るようないくつかの他のシステムを使用し得る。

【００４２】本発明の１つの実施態様によると．複数の開催地に対する電子チケットを生成．格納、および確認するためのシステムおよび方法が与えられる。チケットは．例示的に標準的スマートカード上に格納されるが、３ＣＯＭ　Ｃｏｒｐｏｒａｔｉｏｎによる Ｐａｌｍ Ｐｉｌｏｔ または Ｄａｌｌａｓ　Ｓｅｍｉｃｏｎｄｕｃｔｏｒによる iＢｕｔｔｏｎなどの他のデバイスも意図される。格納されたチケットは．スポーツイベント．娯楽イベント、航空便．および自動車通行料などの、入場券または通行券が予め購入され得る任意の機会に対するものであり得る。本発明の本実施態様によりチケットがスマート上に格納された各開催地は、スマートカード上に格納された関連アプレットを有する。チケット発券共有アプレットがまた格納される。以下に記載されるように、これらのアプレットは、スマートカードとチケット／開催地ロード機能との間およびスマートカードとチケット確認デバイスとの間のインターフェースをとるために使用される。

【００４３】図１は、ユーザのスマートカード上に格納されたチケットを発行、格納、および確認するための本発明の実施態様による例示的システムを図示する。スマートカード１００は、スマートカードに対するＩＳＯ７８１６仕様に例示的に従う。このようなスマートカードは．後に取り出されるための電子データの種々の種類および量を格納することができる。

【００４４】アプレットローダ１０２は、スマートカード１００上へ１つ以上のアプレットをロードする．アプレットローダ１０２によってスマートカード１００上へロードされるアプレットは．スマートカード１００がロードされたアプレットに関連した開催地へのチケットを格納することを可能にする．例えば．１つの開催地アプレットは、Ｓａｎ　Ｆｒａｎｃｉｓｃｏ　Ｇｉａｎｔｓによって開催される野球の試合に対応し得る。このアプレットをロードすることは．スマートカード１００が特定の試合またはある範囲の試合（例えば、シーズンパス）に対するチケットを格納することを可能にする。例示的に、アプレットローダ１０２は．単一開催地に関するアプレットをロードするように構成される。しかし、別の実施態様において、アプレットローダ１０２は、複数の開催地からアプレットをロードする。

【００４５】開催地アプレット（すなわち、個々の開催地に関連したアプレット）に加えて．チケット発券共有アプレットがまた、すべての開催地アプレットによって使用されるためにスマートカード１００上へロードされる．以下に議論されるように、この共有アプレットは、開催地アプレットの各々に共通して利用可能であり、開催地アプレットの各々に代わって使用される機能を与える。

【００４６】チケットローダ１０４は．個々のイベント（またはある範囲のイベント）に対する電子チケットをスマートカード１００上へロードする。各スマートカードは．同じまたは異なるイベント、開催地、および日付などに対する複数のチケットを格納することができる。例示的に、スマートカード１００上へロードされた各チケットは、イベントを開催しチケットを受理する開催地に対応する開催地アプレットに関連して格納される。本実施態様において、開催地のアプレットは、その開催地でのイベントに対するチケットがロードされる前にスマートカード１００上へ（アプレットローダ１０２などによって）ロードされる。

【００４７】例示的に、チケット確認デバイス１０６は．イベントを開催する開催地に位置し、そのイベントに対するチケットがスマートカード１００に格納される。確認デバイス１０６は．チケットが現在のイベントに対するものであることを保証するようにチケットを確

認し．この確認に基づいてチケットを受信する。

【００４８】本発明の本実施態様において、アプレットローダ１０２．チケットローダ１０４．および確認デバイス１０６は．スマートカード１００を受信、読み取り．および書き込みするために備えられた別個の電子システムである。この実施態様において．ユーザは．所望の処理を行うために各システムにスマートカード１００を物理的に提示する。別の実施態様において、アプレットローダ１０２．チケットローダ１０４、および確認デバイス１０６のいずれかまたはすべてが同じシステムに配置する。特に．アプレットローダおよびチケットローダがそうである。

【００４９】本発明のさらに別の実施態様において、アプレットローダ１０２、チケットローダ１０４．および確認デバイス１０６のいずれかまたはすべてがインターネットまたは他のワイドエリアネットワークに接続されたコンピュータシステムを備える。このような実施態様において、これらのシステムは、スマートカード１００を受信、読み取り、および書き込みするために備えられたユーザのコンピュータシステムを介してユーザによってアクセスされる。

【００５０】図２は、チケット発券共有アプレット、複数の開催地アプレット、および複数のチケットが存在するスマートカード１００を図示する。スマートカード１００は、他のデバイス（図１のアプレットローダ１０２．チケットローダ１０４．および確認デバイス１０６など）とインターフェースをとり、スマートカードからの情報の取り出しおよび格納を管理するためのオペレーティングシステム２００を備える。オペレーティングシステム２００は．例示される実施態様において．ロードされたアプレットを動作させるためのＪａｖａ Ｖｉｒｔｕａｌ Ｍａｃｈｉｎｅ（ＪＶＭ）を含む。オペレーティングシステム２００は．スマートカード１００上へロードされたアプレットを確認するための暗号鍵２００ａ（以下「アプレットローダ鍵」と称される）をさらに含む。したがって、アプレット署名２０２ｂ、２１０ｂ．および２２０ｂは、アプレットがロードされたときに．アプレットローダ鍵２００ａを用いて認証される。例示的に、アプレット署名は、関連したアプレットのロードの前またはそれと同時に作成される。

【００５１】チケット発券共有アプレット２０２は、スマートカード１００上にインストールされた種々の開催地アプレットによって要求される命令（例えば．モジュール．オブジェクト、およびファンクションなどの形態をとる）を含む。チケット発券共有アプレット２０２は．各開催地アプレットに共通の機能（チケット確認、チケットローダ１０４および確認デバイス１０６と通信するためのプロトコルなど）を与え．したがって各開催地アプレットのサイズがより小さくなることを可能にし．従ってスマートカード１００上に格納領域を確保できる。例えば．本発明の１つの実施態様において．チケット発券共有アプレット２０２は、チケットをロード、確認．および／またはキャンセル（例えば、イベントへの入場許可を得るためにチケットが使用された後のキャンセル）をするための命令を与える。チケット発券共有アプレット２０２は、以下で記述されるように．個々の開催地アプレットを確認するために暗号鍵２０２ａ（以下「開催地ローダ鍵」と称される）を含む。特に．開催地アプレットがロードされたとき、チケット発券共有アプレット２０２は、各アプレットの開催地署名を認証する。

【００５２】本発明の別の実施態様において、チケット発券共有アプレットは、チケットの詳細を遵守することを強制または確実にするための命令を含む。例えば、このような実施態様において．スマートカード１００は、ユーザがチケットで決められた自分の座席に座っていることを確かめたり、または正しい座席を見つけることを補助するためにイベントにおける客席区域内に配置されるスマートカード読み取り器に挿入され得る。

【００５３】開催地アプレット２１０および２２０は、スマートカード１００上にインストールされている様子が示される。例示的に、開催地アプレット２１０は、ＳａｎＦｒａｎｃｉｓｃｏ Ｇｉａｎｔｓのホームでの野球の試合を表す。開催地アプレット２２０は、例示的にＵｎｉｔｅｄ Ａｉｒｌｉｎｅｓの航空便を表す。開催地アプレット２１０および２２０は．チケットをロードする前にチケットローダ１０４に対し開催地アプレット２１０および２２０を認証するために使用される暗号鍵２１０ａおよび２２０ａ（以下「開催地鍵」と称される）を含む。開催地鍵はまた、関連した開催地に対する．チケットに伴うチケット署名を確認するために使用される。

【００５４】開催地アプレット２１０および２２０はまた．オペレーティングシステム２００に対し開催地アプレットを確認するためのアプレット署名２１０ｂおよび２２０ｂを含む。上述のように、例示的に、アプレット署名は、開催地アプレットのロードの前にまたはそれと同時にアプレットローダ１０２によって作成される。次にオペレーティングシステム２００は．アプレットがロードされたときに、アプレットローダ鍵２００ａを用いてアプレット署名２１０ｂおよび２２０ｂを認証する。

【００５５】開催地アプレット２１０および２２０は、チケット発券共有アプレットに対し開催地アプレットを確認するための開催地署名２１０ｃおよび２２０ｃをさらに含む。アプレット署名２１０ｂおよび２２０ｂと同様に．開催地署名２１０ｃおよび２２０ｃは、開催地アプレット２１０および２２０のインストールの前にまたはそれと同時に作成される。開催地アプレットがロードされたとき、チケット発券共有アプレット２０２は、開催地署名を認証する。

【００５６】チケット２１２、２１４、および２１６は、Ｓａｎ Ｆｒａｎｃｉｓｃｏ Ｇｉａｎｔｓのホームで行われる特定の野球の試合を表す。チケット２２２は、Ｓａｎ ＦｒａｎｃｉｓｃｏからＰｉｔｔｓｂｕｒｇｈ，ＰＡへのＵｎｉｔｅｄＡｉｒｌｉｎｅｓにより提供される特定の航空便を表す。

【００５７】スマートカード１００上に格納された各チケットは、開催イベントに関する情報を含む。したがって、チケット２１２、２１４、および２１６は、試合の日付、対戦相手、および指定座席番号などの情報を含む。本発明の本実施態様において、チケット中に格納された情報は、チケットの認証を確認するためにチケット署名とともに使用される。したがって、チケットに格納された情報の量および種類は、開催地、イベント、およびチケットの種類などに依存して変化する。個々のチケット２１２、２１４、および２１６の代わりに、スマートカード１００の所有者は、例えば、シーズンパスの形態の唯一のチケットを有することがある。シーズンパスチケットは、１日を越えて有効であり、したがってチケット２１２、２１４、および２１６と異なる情報を含む。

【００５８】チケット２１２、２１４、２１６、および２２２はそれぞれ、対応する開催地の鍵を用いてチケットローダ１０４によって生成されたチケット署名（参照符号２１２ａ、２１４ａ、２１６ａ、および２２２ａによって表される）を含む。公開鍵暗号（ＰＫＥ）および非対称鍵ペアを用い、開催地鍵２１０ａおよび２２０ａが開催地公開鍵である本発明の実施態様において、チケット署名は、公開鍵に対応する秘密鍵を使用して生成される。対象鍵（ＤＥＳなど）を使用する別の実施態様において、チケットローダ１０４は、開催地鍵２１０ａおよび２２０ａのコピーを用いて、発行されたチケットの署名をする。上記のように、チケットがスマートカード１００上へロードされたとき、対応する開催地アプレットは、チケット署名をその開催地鍵を用いて認証することによってチケットを確認する。

【００５９】当業者は、スマートカード１００上に格納されたアプレットが、データの秘密を保持し得、したがって他の格納されたアプレットへアクセス不可能であることを理解する。これは、１つのアプレットが、特定の開催地アプレットと関連したチケットに不正を働いたり、または検査したりすることを防止する。しかし、本実施態様において、チケットは、確認デバイス１０６に提示された後にキャンセルまたは使用不可にされる。別の実施態様において、個々のチケットは、削除または上書きされる。

【００６０】アプレットのロード

本発明の本実施態様において、スマートカード１００上にロードされる開催地アプレットおよびチケット発券共有アプレットは、実行可能なコンピュータプログラムまたは実行可能なコンピュータコードのモジュールを含む。本発明の本実施態様において、チケット発券共有アプレットは、スマートカード間で実質的に同一である。各開催地の開催地アプレットは同様に、開催地鍵およびロードされ得る任意のチケットを除いて、スマートカード間で同様である。

【００６１】本発明の１つの実施態様において、開催地アプレットは、標準的な方法によって構成されたＪａｖａアプリケーションを含む。例えば、Ｊａｖａプログラミング命令を含むファイルは、バイナリクラスファイルを形成するためにＪａｖａコンパイラを用いてコンパイルされる。次に、クラスファイルは、スマートカードアプリケーションファイルに変換される。この変換プロセス中に、カードアプリケーションファイルは、暗号化の種類（例えば、対称または非対称）に依存して、アプレットローダ鍵２００ａ（図２に示す）またはその相補形を使用してデジタル的に署名される。

【００６２】図３は、署名されたカードアプリケーションファイル（例えば、図２のアプレット２１０）がアプレットローダ１０２からスマートカード１００上へロードされる例示的なプロセスを図示する。本発明の本実施態様において、アプレットローダ１０２は、チケット販売機であり、チケットローダ１０４と同じ場所に配置される。この実施態様において、開催地アプレット２１０は、Ｇｉａｎｔｓの野球チケットが購入されたときに、アプレットがまだスマートカード１００上になければ、自動的にロードされる。また、この実施態様において、チケット発券共有アプレット２０２は、スマートカード１００上になければ自動的にロードされる。別の実施態様において、チケット発券共有アプレット２０２および開催地アプレット２１０のいずれか一方または両方が、スマートカードが製造される時点またはそれが販売される時点で、スマートカード上に予めロードされる。

【００６３】ここで図３を参照すると、状態３００は開始状態である。状態３０２において、アプレットローダ１０２は、スマートカード１００に結合され、アプレット２１０をダウンロードする準備をする。例示的に、スマートカード１００の所有者は、アプレットローダ１０２を含むデバイスへスマートカードを挿入し、アプレット２１０のインストールを選択する（例えば、Ｇｉａｎｔｓの野球チケットの購入を希望することによって）。別の実施態様において、所有者は、インターネットまたは他の通信リンクを介してアプレットローダ１０２に接続された別個のコンピュータシステムにスマートカード１００を挿入する。

【００６４】状態３０４において、スマートカード１００は、アプレットをロードする準備がなされたことを示し、そして、本実施態様においては、現在の構成に関する情報（どのアプレットがロードされるか、どのバージョンのオペレーティングシステムおよびＪａｖａ Ｖｉ

ｒｔｕａｌ　Ｍａｃｈｉｎｅがインストールされるかなどの情報）をアプレットローダに渡す。１つの実施態様において、スマートカード１００は、アプレットを受信する用意ができたことを示す前に自己チェックを行う。例示的に、自己チェックは、データを格納および取り出すカードの能力を試験し、不良なまたは損壊のあるメモリセルを試験する。スマートカードによってアプレットローダ１０２へ転送された情報は、カード上で利用できる格納領域の量を含み得る。選択されたアプレットをロードするための領域が不十分な場合、エラーメッセージがユーザに示される。

【００６５】状態３０６において、アプレットローダ１０２は、チケット発券共有アプレット２０２がすでにスマートカード１００上に存在するかどうかを判断する。上記のように、チケット発券共有アプレット２０２は、開催地アプレット２１０および他の開催地アプレットによって使用される命令を含む。例示的に、この判断は、状態３０４においてスマートカード１００によってアプレットローダ１０２へ返された情報に基づいてなされる。

【００６６】状態３０６においてチケット発券共有アプレット２０２がスマートカード１００上にインストールされていないと判断される場合、プロセスは、状態３１０へ続く。そうでない場合は、状態３０８において開催地アプレット２１０がすでにスマートカード１００上にロードされているかどうか判断される。ロードされていなければ、プロセスは、状態３１６に進む。しかし、両方のアプレットがすでにロードされていれば、プロセスは終了状態３２０へ進む。

【００６７】状態３１０において、チケット発券共有アプレットは、まだ署名されていなければ、アプレットローダ鍵２００ａに相補的な暗号鍵（例えば、非対称暗号システムを使用する場合、「秘密」鍵は「公開」鍵２００ａに対応する）を用いて署名され（例えば、アプレットローダ１０２によって）、アプレット署名２０２ｂ（図２参照）を作成する。次に、署名されたアプレットは、スマートカード１００にダウンロードされる。例示的に、アプレットは、何バイトかの複数のストリーム（例えば、各ストリーム中約２００バイト）でスマートカード上にダウンロードおよび格納され、各ストリームは、関連したチェックサムによって確認される。状態３１２において、スマートカードは、アプレットの正確な受信を確認し、状態３１４においてインストールが成功したかしていないかをアプレットローダに通知する。共有アプレット２０２が正しくロードされていなかったならば、エラーメッセージが返され、プロセスは、終了状態３２０で終了する。

【００６８】チケット発券共有アプレット２０２のインストールが成功すれば、または開催地アプレット２１０がロードされていないと状態３０８において判断されるならば、プロセスは状態３１６に進む。

【００６９】状態３１６において、開催地アプレット２１０は、アプレットローダ１０２によって署名され（まだ署名されていなければ）、アプレット署名２１０ｂおよび／または開催地署名２１０ｃを作成し、そして次にアプレットローダ１０２からスマートカード１００上へダウンロードされる。以下に議論されるように、開催地鍵２１０ａは、チケットローダ１０４に対する開催地アプレット２１０を認証するためおよびチケットローダからロードされたチケットを確認するために使用される。好ましい暗号安全性の種類（例えば、対称または非対称鍵）に依存して、アプレット署名２１０ｂおよび開催地署名２１０ｃは、アプレットローダ鍵２００ａおよび開催地ローダ２０２ａ、またはその相補形をそれぞれ用いて作成される。

【００７０】状態３１８において、スマートカード１００は、ダウンロードされたアプレットを確認し、アプレットのロードが成功したかまたはエラーが起きたかをアプレットローダに示す。例示的に、スマートカード１００は、チェックサムを計算しそれをアプレットローダ１０２によって与えられたチェックサムと比較することによってアプレットの受信が成功したことを確認する。別の実施態様において、ダウンロードされたアプレットのアプレット署名２１０ｂは、署名の作成に使用された鍵の形態に対応する暗号技術を用いて確認される。１つの特定のこのような実施態様において、スマートカード１００は、アプレットからのハッシュ値を計算し、その値と署名から取り出されたハッシュ値とを比較する。この２つのハッシュ値が一致すれば、スマートカードはアプレットが完全な状態で受信されたと考える。同様のプロセスを使用して、チケットがダウンロードされた場合にチケット署名を確認する。次いでプロセスは、終了状態３０２で終了する。

【００７１】チケットのロード

一旦開催地アプレットがスマートカード１００上へロードされると、その開催地でのイベント（スポーツ競技場での競技または試合、航空会社によって提供される航空便など）に対するチケットは購入され、同様にロードされ得る。本発明の本実施態様において、開催地アプレット、チケット発券共有アプレット２０２、および関連チケットは、互いに併せあって、組合わせられたチケット／アプレットローダから必要に応じてロードされる。

【００７２】図４は、チケットローダ１０４からＧｉａｎｔｓの野球の試合（これのための開催地アプレット２１０がインストールされている）に対する電子チケットを購入し、電子チケットをスマートカード１００上にインストールするための例示的な手続きを図示する。本発明の本実施態様において、チケットローダ１０４は、インターネットなどの公衆通信回線に接続されたウエブサーバの一部である。この実施態様において、スマートカ

ード１００は、スマートカード１００の所有者によって操作されるコンピュータシステムに結合される。このコンピュータシステムはまた、インターネットに接続される。チケットは、開催地のウェブサーバに対するインターフェースを使用して選択され、次にインターネットを介してダウンロードされ、スマートカード１００上に格納される。

【００７３】ここで図４を参照すると、状態４００が開始状態である。状態４０２において、スマートカード１００の所有者は、チケット購入／ロード手続きを開始する。本発明の１つの実施態様において、所有者は、第１に、チケットを希望するイベントを選択する。ここで記述の実施態様において、例えば、野球の試合は、所望の座席の番号および種類とともに特定される。別の例として、所有者は、航空路線予約代理人に対して所有者が搭乗を希望する航空便（日付、時刻、およびおそらく座席を含む）を特定する。スマートカードの所有者が開催地／イベントを選択し、そのイベントに関する任意の必要事項または基準を特定した後に、所有者は、そのように構成されたチケットの受信を合図する。

【００７４】状態４０４において、チケットローダ１０４は、スマートカードおよび／または開催地アプレット２１０を認証するために、自分自身を識別し、スマートカード１００にチャレンジする。例示的に、チャレンジは、チケットローダ１０４によってスマートカード１００へ送信された乱数の形態をとる「ゼロ知識証明（ｚｅｒｏ ｋｎｏｗｌｅｄｇｅ ｐｒｏｏｆ）」である。開催地アプレット２１０は、開催地鍵２１０ａ用いてデジタル署名を生成し、そして結果をチケットローダ１０４に戻すことによってチャレンジを満たす。別の実施態様において、開催地アプレット２１０は、開催地鍵２１０ａを用いて乱数を暗号化し、そして結果をチケットローダ１０４に戻すことによって、状態４０６においてチャレンジを満たす。

【００７５】状態４０８において、チケットローダ１０４は、スマートカード１００から受け取られた署名を確認する。この確認の目的のために、チケットローダ１０４は、開催地鍵２１０ａに対して相補形の鍵を有する。例えば、開催地鍵２１０ａが関連する開催地の公開鍵である。非対称鍵（例えば、ＲＳＡ）を使用する本発明の実施態様において、チケットローダ１０４は、対応する秘密鍵を有する。対称鍵（例えば、デジタル暗号基準）を使用する本発明の実施態様において、チケットローダ１０４および開催地アプレット２１０は、同じ鍵のコピーを有する。確認の試みが失敗すれば、チケットロードプロセスは、実施および安全性の関係に依存して、チャレンジ／確認手続きを再度試みるか（制限回数まで）、または失敗しそしてエラーを報告するかのいずれかを行う。

【００７６】次に、状態４１０において、チケットローダ１０４は、スマートカードの所有者／ユーザによって選択されたイベントデータに基づいて開催地に対するチケット２１２を生成および署名する。例示的に、チケットローダ１０４は、開催地アプレット２１０が状態４０８において確認されたのと同じ鍵を使用してチケット２１２に署名する。状態４１２において、署名２１２ａで署名を完了したチケット２１２が、スマートカード１００上にダウンロードおよび格納される。

【００７７】状態４１４において、開催地アプレット２１０は、開催地鍵２１０ａを用いて署名２１２ａを認証することによって、ダウンロードされたチケット２１２を確認し、そして状態４１６において、成功または失敗を示すメッセージを用いて応答する。本発明の別の実施態様において、開催地鍵２１０ａと異なる第２の開催地鍵が、ダウンロードされたチケットを確認する目的のために開催地アプレット２１０とともに格納される。手続きは、終了状態４１８で終了する。

【００７８】ここで記述の実施態様において、上記プロセスに続いて、各チケットがチケットローダ１０４からダウンロードされなければならない。別の実施態様において、複数のチケットが、一度に１つの開催地に対して、選択、処理、およびダウンロードされ得る。

【００７９】チケット確認

本発明の本実施態様において、チケットは、適切な開催地での受信のために提示される場合に、確認デバイス１０６によって確認される。図５は、本発明の本実施態様による、チケット２１２を確認するための例示的手続きを図示する。

【００８０】状態５００は、開始状態である。状態５０２において、ユーザは、チケット２１２において特定される野球の試合への入場許可を得るために、スマートカード１００を確認デバイス１０６へ提示する。例示的に、確認デバイス１０６は、スマートカード１００を受け取り、それと通信するように構成されたコンピュータシステムを含む。

【００８１】状態５０４において、確認デバイス１０６は、上記チケットロード手続きにおいて行われたように、スマートカード１００に対するチャレンジを生成および発行する。スマートカード１００に与えられる乱数は、状態５０６において、開催地鍵２１０ａを使用して、開催地アプレット２１０によって署名される。状態５０８において、確認デバイスが開催地鍵２１０ａに相補形の鍵を使用して署名を認証する。チャレンジとともに戻された署名を認証することによって、確認デバイス１０６は、開催地アプレット２１０を確認できる。

【００８２】署名を認証した後に、状態５１０において、確認デバイス１０６は、スマートカード１００によって保持されるチケットデータを要求する。開催地アプレット２１０は、状態５１２において、チケット２１２（例えば、チケットデータおよび署名）を確認デバイス

１０６に送信する。例示的に、確認デバイス１０６は、日付、時刻、および／または他の識別データによって識別される、現在のイベントに対して使用可能な格納されたチケットだけが通知される。本発明の１つの実施態様において、チケット発券共有アプレット２０２は、確認デバイス１０６に対して特定されるチケットを決定する（例えば、どの開催地－したがってどの開催地アプレットおよびチケット－が確認デバイスに対応するかを決定することによって）。あるいは、開催地アプレット２１０および確認デバイス１０６は、現在の開催地に関連した複数のチケットのうちのどれが使用されるべきかを決定するために、通信する。

【００８３】状態５１４において、確認デバイス１０６は、チケットデータを確認し（例えば、日付、時刻、参加チーム、および座席番号を確かめる）、チケット署名を認証する。チケットデータおよび署名が検査を通過すれば、スマートカード１００は、チケット２１２をキャンセルまたは消去するように命令され、ユーザは許可される。

【００８４】本発明のここで記述の実施態様において、チケット２１２は、スマートカード１００上にロードされた将来のチケットを用いて上書きされる。別の実施態様において、チケットは、消去も上書きもされない。

【００８５】１つのスマートカード上にある複数の開催地のための電子チケットを格納および確認するためのシステムおよび方法が提供される。本実施態様によると、スマートカードのオペレーティングシステムは、Ｊａｖａ Ｖｉｒｔｕａｌ Ｍａｃｈｉｎｅおよびアプレットローダ鍵を含む。開催地ローダ鍵を含む共有アプレットは、アプレットローダ鍵を用いて確認され、スマートカード上に格納される。１つ以上の開催地アプレットがまた、関連する開催地に対応するそれぞれの開催地鍵とともにスマートカード上に格納される。各開催地アプレットは、アプレットローダ鍵および開催地ローダ鍵によって確認される。共有アプレットは、チケットローダおよびチケット確認デバイスとのインターフェースをとるために開催地アプレットによって使用される。チケットは、開催地アプレットに関連するイベントに対して購入され、関連する開催地アプレットに関連してスマートカード上に格納される。チケット署名は、各開催地アプレット開催地鍵を用いて認証される。チケットは、イベントへの入場許可を得るために提出された後にキャンセルされる。

【００８６】本発明の実施態様の前述の記載は、例示および説明だけの目的で提示された。例示および記載は、あらゆる実施例を説明し尽くすものでもなければ、本発明を開示された形態に限定することを意図しない。多くの改変および変更が当業者にとって明らかである。したがって、上記開示は本発明を限定することを意図せず、本発明の範囲は、添付の請求の範囲によって規定される。

【００８７】

【発明の効果】単一の電子デバイス（スマートカード、および携帯コンピュータなど）上に複数の開催地で提供されるイベントに対する電子チケットを格納するためのシステムおよび方法が提供される。これにより、紙のチケットの発行を必要がなくなり、さらに、多くのイベントに参加する場合、多くの紙のチケットを持参する必要がなくなる。

【図面の簡単な説明】

【図１】スマートカードが開催地アプレットおよび開催地への入場のためのチケットを格納するために使用される、本発明の実施態様によるシステムを図示する１つのブロック図である。

【図２】複数の開催地アプレットおよびチケットを含む、本発明の実施態様によるスマートカードを図示する図である。

【図３】スマートカード上に開催地アプレットをロードする、本発明の実施態様による１つの方法を示すフローチャートである。

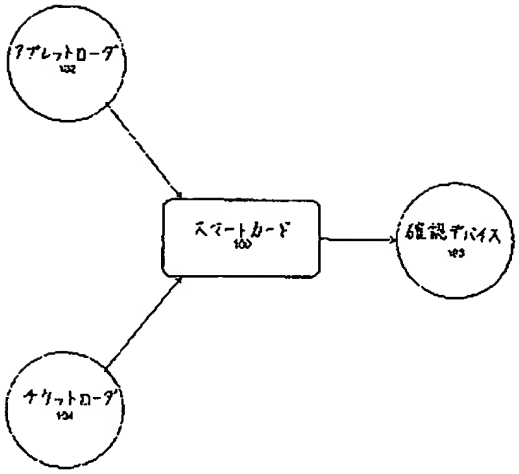
【図４】スマートカード上にチケットをロードする、本発明の実施態様による１つの方法を示すフローチャートである。

【図５】スマートカード上に格納されたチケットを確認する、本発明の実施態様による１つの方法を示すフローチャートである。

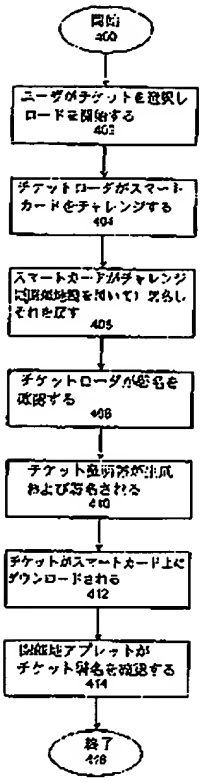
【符号の説明】

１００　スマートカード
１０２　アプレットローダ
１０４　チケットローダ
１０６　確認デバイス

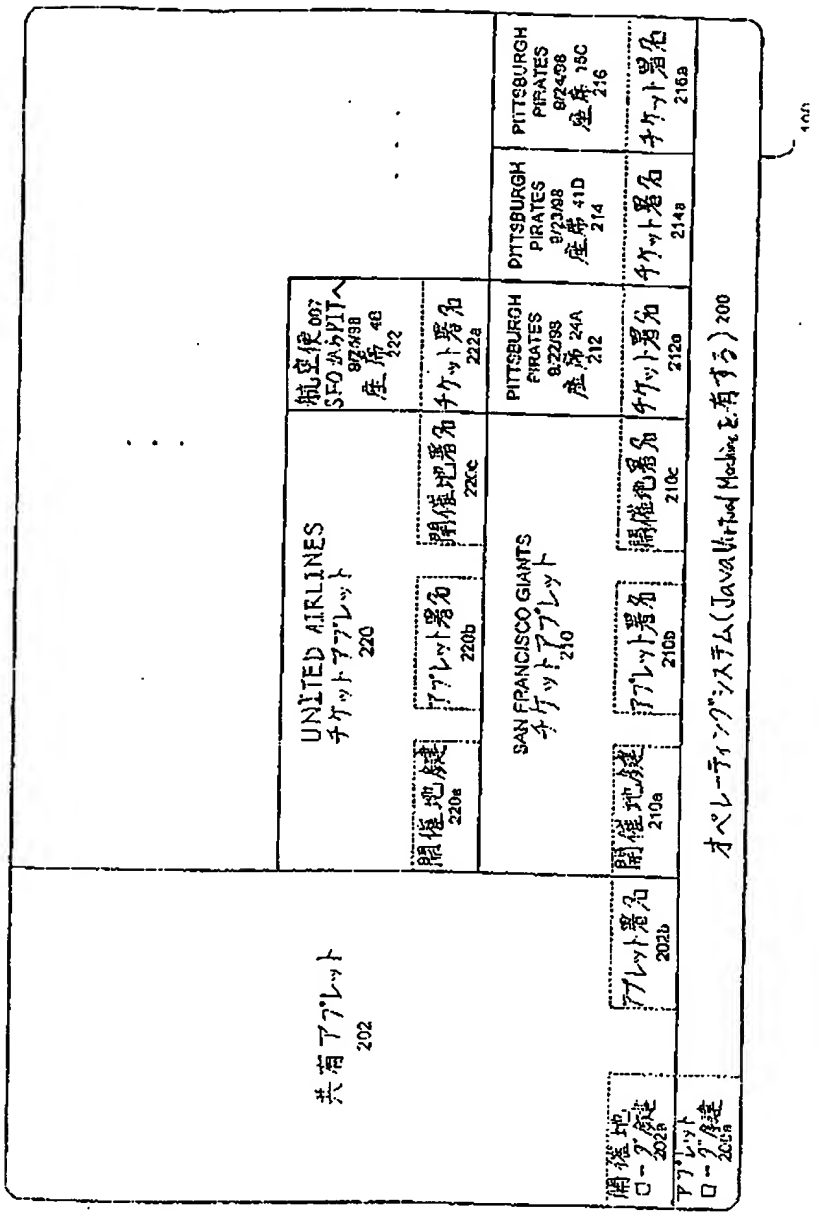
【図１】


アプレットローダ
132
スマートカード
100
確認デバイス
103
チケットローダ
134

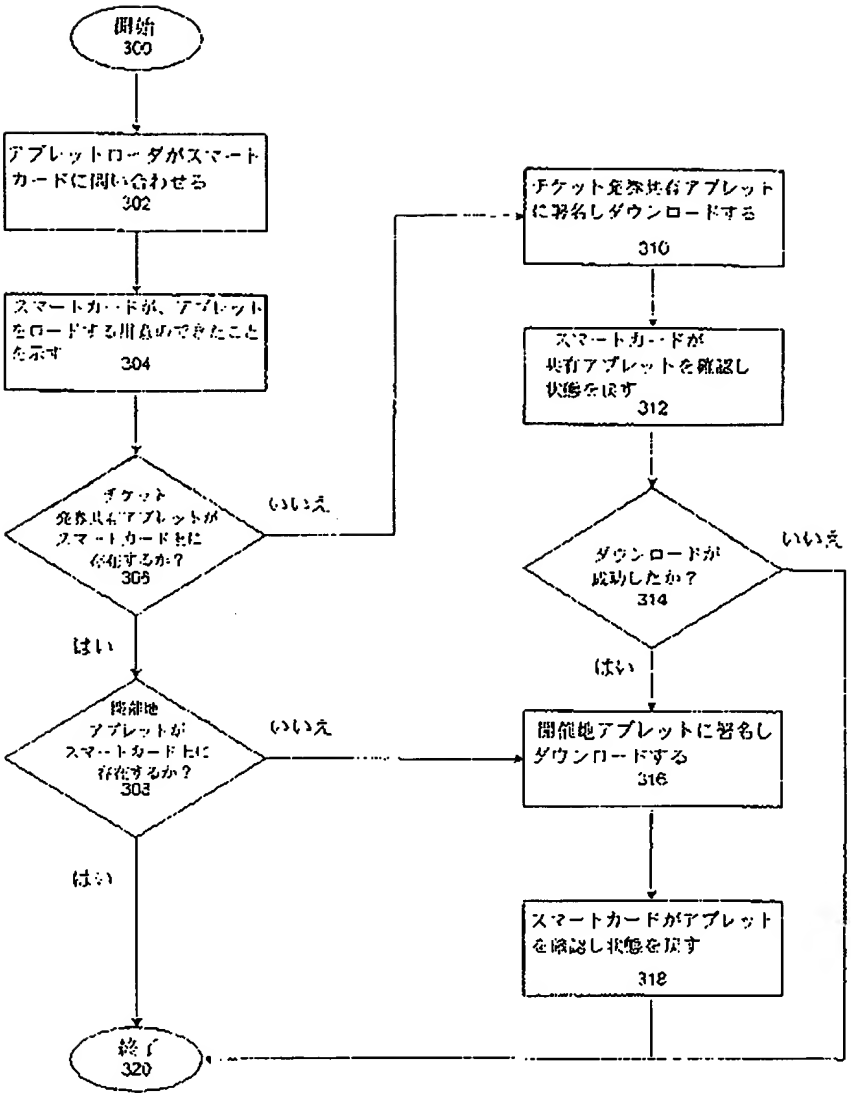
【図４】


開始
400
ユーザがチケットを選択しロードを開始する
402
チケットローダがスマートカードをチャレンジする
404
スマートカードがチャレンジに関数値を用いて署名しそれを返す
406
チケットローダが署名を返信する
408
チケット登録署名が生成および署名される
410
チケットがスマートカード上にダウンロードされる
412
関数値アプレットがチケット署名を検証する
414
終了
416

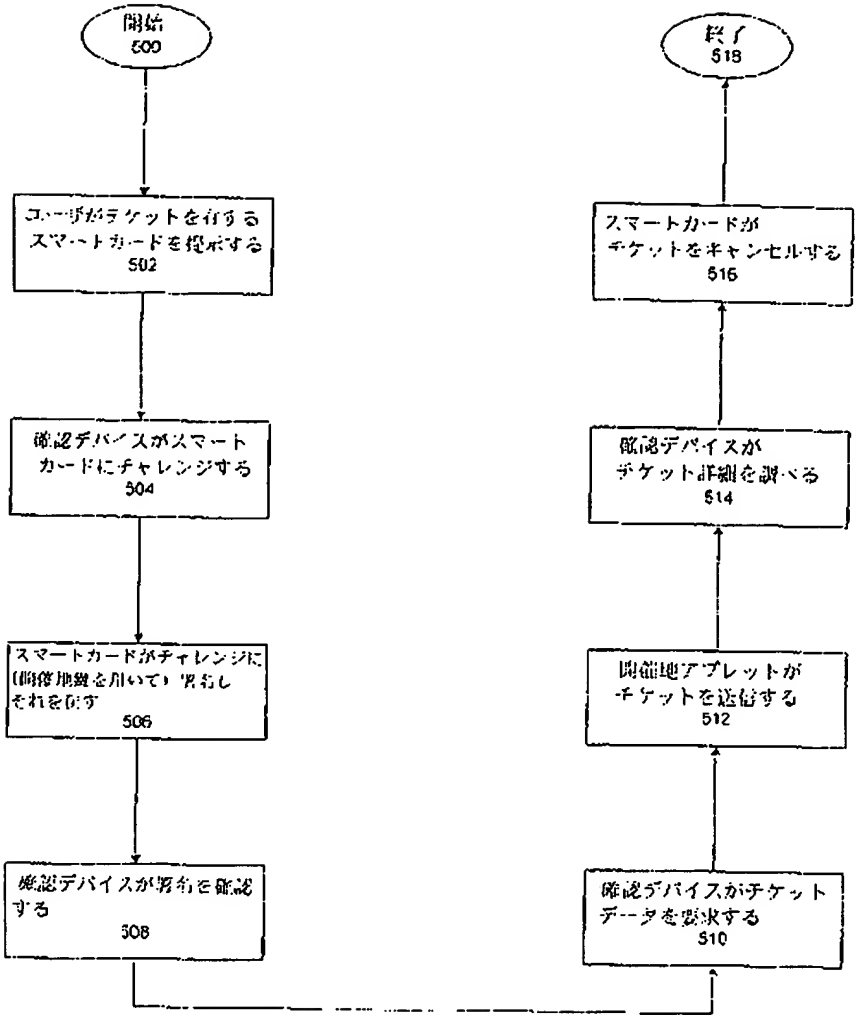
【図2】


共有アプレット
202
開催地ロータ解決
202a
アプレット署名
202b
オペレーティングシステム(Java Virtual Machine を有する) 200
UNITED AIRLINES
チケットアプレット
220
開催地解決
220a
アプレット署名
220b
開催地署名
220c
航空便 007
SFO JAN PIT へ
9/23/98
座席 48
222
チケット署名
222a
SAN FRANCISCO GIANTS
チケットアプレット
210
開催地解決
210a
アプレット署名
210b
開催地署名
210c
チケット署名
212a
PITTSBURGH
PIRATES
8/22/98
座席 24A
212
PITTSBURGH
PIRATES
8/23/98
座席 41D
214
チケット署名
214a
PITTSBURGH
PIRATES
8/24/98
座席 15C
216
チケット署名
216a

【図3】


開始
300
アプレットローダがスマートカードに問い合わせる
302
スマートカードが、アプレットをロードする用意ができたことを示す
304
チケット発券共有アプレットがスマートカードに存在するか？
305
いいえ
はい
開催地アプレットがスマートカードに存在するか？
308
いいえ
はい
チケット発券共有アプレットに署名しダウンロードする
310
スマートカードが共有アプレットを確認し状態を返す
312
ダウンロードが成功したか？
314
いいえ
はい
開催地アプレットに署名しダウンロードする
316
スマートカードがアプレットを確認し状態を返す
318
終了
320

【図5】



フロントページの続き

(72)発明者 セオドール チャールズ ゴールドスタイン
アメリカ合衆国 カリフォルニア 94306, パロ アルト, ラバラ アベニュー 875

(72)発明者 ジョナサン ビー. ジエグラー
アメリカ合衆国 カリフォルニア 95014, クペルティノ, サンタ ルシア ロード 10611

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.